Features

- A Family of Devices with User Memories of 1 Kbit to 64 Kbit
- Contactless 13.56 MHz RF Communications Interface
  - ISO/IEC 14443-2:2001 Type B Compliant
  - ISO/IEC 14443-3:2001 Type B Compliant Anticollision Protocol
  - Tolerant of Type A Signaling for Multi-Protocol Applications
- Integrated 82 pF Tuning Capacitor
- User EEPROM Memory Configurations:
  - 64 Kbits Configured as Sixteen 512 byte (4 Kbit) User Zones [AT88SC6416CRF]
  - 32 Kbits Configured as Sixteen 256 byte (2 Kbit) User Zones [AT88SC3216CRF]
  - 16 Kbits Configured as Sixteen 128 byte (1 Kbit) User Zones [AT88SC1616CRF]
  - 8 Kbits Configured as Eight 128 byte (1 Kbit) User Zones [AT88SC0808CRF]
  - 4 Kbits Configured as Four 128 byte (1 Kbit) User Zones [AT88SC0404CRF]
  - 2 Kbits Configured as Four 64 byte (512 bit) User Zones [AT88SC0204CRF]
  - 1 Kbits Configured as Four 32 byte (256 bit) User Zones [AT88SC0104CRF]
  - Byte, Page, and Partial Page Write Modes
  - Self Timed Write Cycle
- 256 byte (2 Kbit) Configuration Memory
  - User Programmable Application Family Identifier (AFI)
  - User-defined Anticollision Polling Response
  - User-defined Keys and Passwords
- High Security Features
  - Selectable Access Rights by Zone
  - 64-bit Mutual Authentication Protocol (under license of ELVA)
  - Encrypted Checksum
  - Stream Encryption
  - Four Key Sets for Authentication and Encryption
  - Four or Eight 24-bit Password Sets
  - Password and Authentication Attempts Counters
  - Anti-tearing Function
  - Tamper Sensors
- High Reliability
  - Endurance : 100,000 Write Cycles
  - Data Retention : 10 Years

CryptoRF Specification

AT88SC0104CRF
AT88SC0204CRF
AT88SC0404CRF
AT88SC0808CRF
AT88SC1616CRF
AT88SC3216CRF
AT88SC6416CRF

5276A–RFID–07/08

1. Introduction

1.1 Description

The CryptoRF® family integrates a 13.56 Mhz RF interface with CryptoMemory® security features. This product line is ideal for RF tags and contactless smart cards that can benefit from advanced security and cryptographic features. The device is optimized as a contactless secure memory for secure data storage without the requirement of an internal microprocessor.

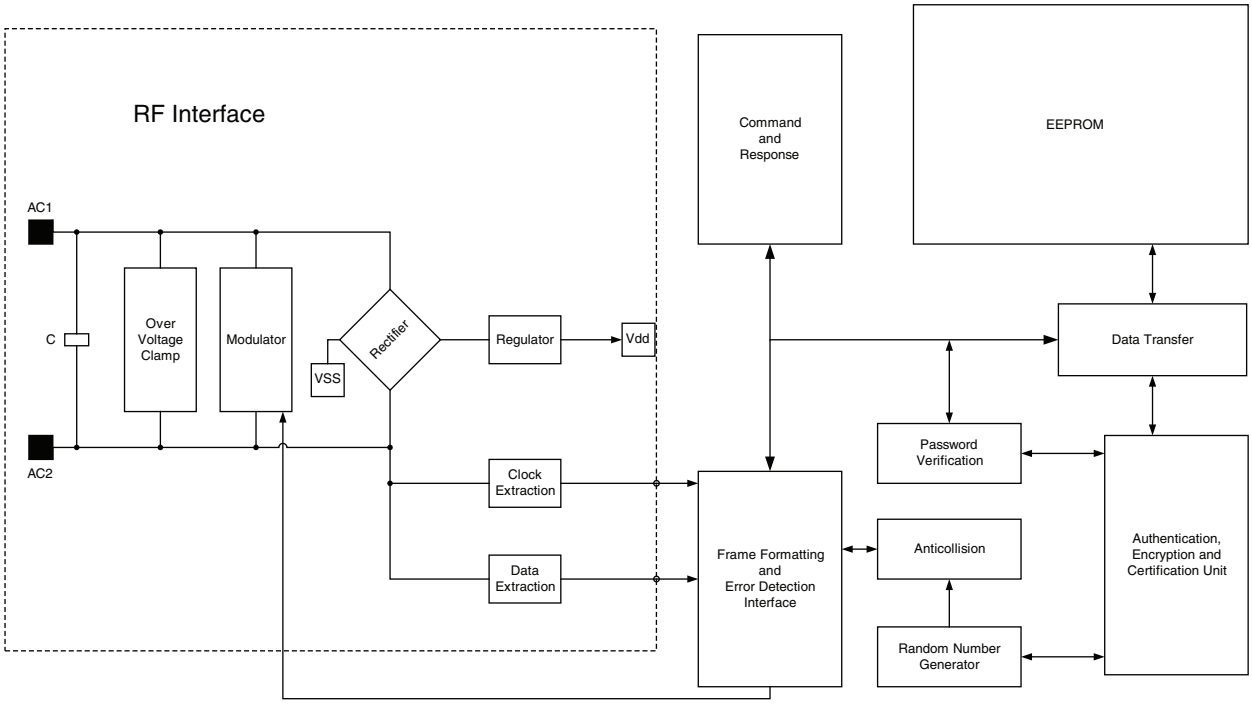
For communications the RF interface utilizes the ISO/IEC 14443–2 and –3 Type B bit timing and signal modulation schemes, and the ISO/IEC 14443-3 Slot-MARKER Anticollision Protocol. Data is exchanged half duplex at a 106k bit per second rate, with a two byte CRC_B providing error detection capability. The RF interface powers the other circuits, no battery is required. Full compliance with the ISO/IEC 14443 –2 and –3 standards results in anticollision interoperability with the AT88RF020 2 Kbit RFID EEPROM product and provides both a proven RF communication interface, and a robust anticollision protocol.

The seven products in this family contain 1 Kbits to 64 Kbits of User Memory plus 2 Kbits of Configuration Memory. The 2 Kbits of Configuration Memory contains read/write password sets, four crypto key sets, security access registers for each user zone, and password/key registers for each zone.

The CryptoRF command set is optimized for a multicard RF communications environment. A programmable AFI register allows this IC to be used in numerous applications in the same geographic area with seamless discrimination of cards assigned to a particular application during the anticollision process.

1.2 Block Diagram

Figure 1-1. Block Diagram



1.3 Communications

All personalization and communication with this device is performed through the RF interface. The IC includes an integrated tuning capacitor, enabling it to operate with only the addition of a single external coil antenna.

The RF communications interface is fully compliant with the electrical signaling and RF power specifications in ISO/IEC 14443-2 for Type B only. Anticollision operation and frame formatting are compliant with ISO/IEC 14443-3 for Type B only.

1.4 Scope

This *CryptoRF Specification* document includes all specifications for the normal mode of CryptoRF operation. This document may be freely distributed without any formal user agreements. The Authentication and Encryption modes of operation are not described in this document.

The Authentication and Encryption modes specifications are described in the document *CryptoRF Specification Addendum for Secure Applications*, which is available only under Non-Disclosure and Limited Licensing Agreements (NDA and LLA). Contact your regional Atmel sales office to obtain this secure document.

1.5 Conventions

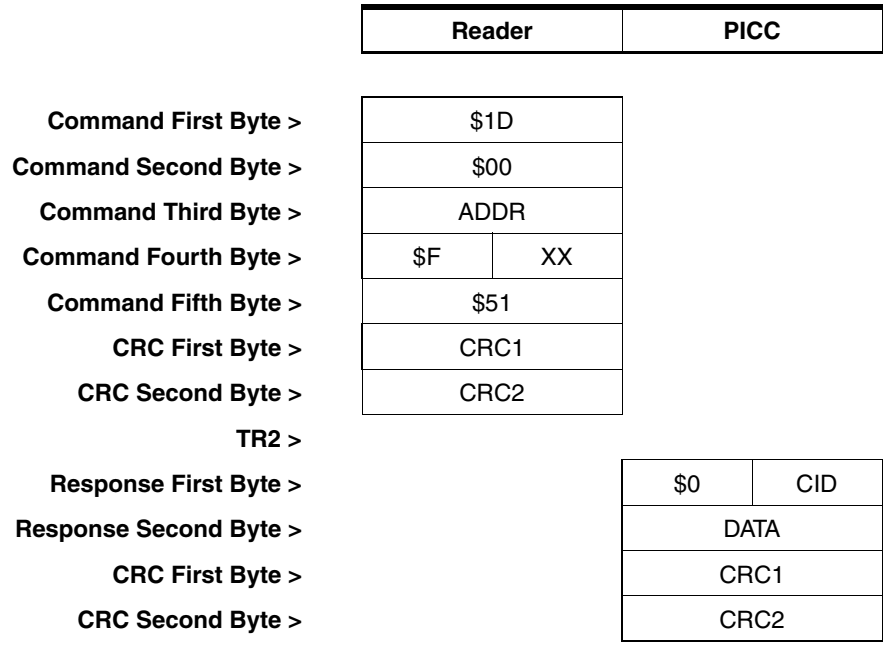
ISO/IEC 14443 nomenclature is used in this specification where applicable. The following abbreviations are utilized throughout this document. Additional terms are defined in Annex A.

- **PCD:** Proximity Coupling Device – is the reader/writer and antenna.
- **PICC:** Proximity Integrated Circuit Card – is the tag/card containing the IC and antenna.
- **RFU:** Reserved for Future Use – is any feature, memory location, or bit that is held as reserved for future use by the ISO standards committee or by Atmel.
- **$xx:** Hexadecimal Number – denotes a hex number “xx” (Most Significant Bit on left).
- **xxxxb:** Binary Number – denotes a binary number “xxxx” (Most Significant Bit on left).

Each command / response exchange between the PCD and PICC is formatted as shown in Figure 1-2. The bytes are shown in the order in which they are transmitted, with PCD transmissions in the left column, and PICC transmissions in the right column.

Each byte contains one or more fields as indicated by lines drawn vertically within the byte. The field in the left half of the byte is the upper nibble of the byte, and the field to the right is the lower nibble of the byte. In Figure 1-2, five fields contain values ($1D, $00, $F, $51, $0), four fields contain field names (“Addr”, “XX”, “CID”, “Data”), and four fields contain error detection codes (CRC1, CRC2).

Figure 1-2. Example Command and Response Format



The CRC error detection codes are calculated using all of the previous bytes in the command or response and are appended to each command and response to allow detection of RF communication errors. These bytes are required by ISO/IEC 14443-3:2001 and are usually calculated and verified in the reader hardware.

2. User Memory

The User EEPROM Memory characteristics are summarized in Table 2-1 below. User Memory is divided into equally sized User Zones. Access to the User Zones is allowed only after security requirements have been met. These security requirements are defined by the user in the configuration memory during personalization of the device. The default configuration is open read/write access to all user memory zones.

Table 2-1. CryptoRF User Memory Characteristics

CryptoRF Part Number	User Memory Size		User Memory Organization		Write Characteristics	
	Bits	Bytes	# Zones	Bytes/Zone	Standard Write	Anti-Tearing Write
AT88SC0104CRF	1K	128	4	32	1 to 16 Bytes	1 to 8 Bytes
AT88SC0204CRF	2K	256	4	64	1 to 16 Bytes	1 to 8 Bytes
AT88SC0404CRF	4K	512	4	128	1 to 16 Bytes	1 to 8 Bytes
AT88SC0808CRF	8K	1K	8	128	1 to 16 Bytes	1 to 8 Bytes
AT88SC1616CRF	16K	2K	16	128	1 to 16 Bytes	1 to 8 Bytes
AT88SC3216CRF	32K	4K	16	256	1 to 32 Bytes	1 to 8 Bytes
AT88SC6416CRF	64K	8K	16	512	1 to 32 Bytes	1 to 8 Bytes

3. Configuration Memory

The configuration memory consists of 2048 bits of EEPROM memory used for storing system data, passwords, keys, codes, and access control registers for each user zone. Access rights to the configuration memory are defined in the control logic and cannot be altered by the user. These access rights include the ability to program certain portions of the configuration memory and then lock the data written through use of the security fuses. The Read System Zone and Write System Zone commands are used to access the configuration memory.

Table 3-1. Configuration Memory Characteristics

CryptoRF Part Number	Password Sets	Key Sets	OTP Memory	Transport Password	
			Free For Customer Use	PW Index	Password
AT88SC0104CRF	4 Sets	4 Sets	27 Bytes	$07	$10 14 7C
AT88SC0204CRF	4 Sets	4 Sets	27 Bytes	$07	$20 C2 8B
AT88SC0404CRF	4 Sets	4 Sets	27 Bytes	$07	$30 1D D2
AT88SC0808CRF	8 Sets	4 Sets	27 Bytes	$07	$40 7F AB
AT88SC1616CRF	8 Sets	4 Sets	27 Bytes	$07	$50 44 72
AT88SC3216CRF	8 Sets	4 Sets	27 Bytes	$07	$60 78 AF
AT88SC6416CRF	8 Sets	4 Sets	27 Bytes	$07	$70 BA 2E

4. Command Set

The CryptoRF command set contains two types of commands: Anticollision commands, and Active State commands. Anticollision commands are explicitly defined in ISO/IEC 14443-3:2001. The CryptoRF Active State commands are Atmel defined commands that are compliant with the ISO/IEC 14443-3:2001 requirements.

The CryptoRF Active State commands contain the CID code that is assigned to a card when it is selected during the anticollision process. See the ATTRIB command for coding of the CID bits.

Table 4-1. Coding of the Command Byte for the Anticollision Command Set

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Command Name	Hexidecimal
0	0	0	0	0	1	0	1	REQB/WUPB	$05
Slot Number				0	1	0	1	Slot MARKER	$s5
0	0	0	1	1	1	0	1	ATTRIB	$1D
0	1	0	1	0	0	0	0	HLTB	$50

Table 4-2. Coding of the Command byte for the CryptoRF Active State Command Set.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Command Name	Hexidecimal
CID				0	0	0	1	Set User Zone	$c1
CID				0	0	1	0	Read User Zone	$c2
CID				0	0	1	1	Write User Zone	$c3
CID				0	1	0	0	Write System Zone	$c4
CID				0	1	1	0	Read System Zone	$c6
CID				1	0	0	0	Verify Crypto	$c8
CID				1	0	0	1	Send Checksum	$c9
CID				1	0	1	0	DESELECT	$cA
CID				1	0	1	1	IDLE	$cB
CID				1	1	0	0	Check Password	$cC
All Other Values Are Not Supported									

4.1 Anticollision Command Definitions

Commands in this section are arranged in order by the hexadecimal code in the command byte.

4.2 REQB / WUPB Polling Commands [$05]

The REQB / WUPB command is used to search for PICCs in the RF field. The command and response are ISO/IEC 14443-3:2001 compliant.

	Reader	PICC
Command >	$05	
	AFI	
	PARAM	
	CRC1	
	CRC2	

ATQB Response >	$50	SUCCESS RESPONSE
	PUPI 0	System Zone Byte $00
	PUPI 1	System Zone Byte $01
	PUPI 2	System Zone Byte $02
	PUPI 3	System Zone Byte $03
	APP 0	System Zone Byte $04
	APP 1	System Zone Byte $05
	APP 2	System Zone Byte $06
	APP 3	System Zone Byte $07
	Protocol 1	$00
	Protocol 2	System Zone Byte $08
	Protocol 3	$51
	CRC1	
	CRC2	

4.2.1 Operation

The “Request B” (REQB) and “Wake-Up B” (WUPB) commands are used to probe the RF field for Type B PICCs as the first step in the anticollision process. The response to an REQB or WUPB command is the “Answer to Request B” (ATQB). PICCs in the Active State are not permitted to answer this command.

4.2.2 Command Field Descriptions

AFI: The Application Family Identifier (AFI) is used to select the family and sub-family of cards which the PCD is targeting. Only PICCs with a matching AFI code are permitted to answer an REQB or WUPB command. Table 4-3 describes the AFI matching criteria. An AFI of $00 activates all Type B PICCs.

Table 4-3. AFI matching criteria for polling commands received by the PICC.

AFI High Bits	AFI Low Bits	REQB/WUPB Polling produces a PICC response from:
$0	$0	All Families and sub-families
“X”	$0	All sub-families of Family “X”
“X”	“Y”	Only sub-family “Y” of Family “X”
$0	“Y”	Proprietary sub-family “Y” Only

“Y” = $1 to $F

“X” = $1 to $F

PARAM: The PARAM byte is used to send two parameters to the PICC. The parameter “N”, which assigns the number of anticollision slots, and the REQB / WUPB selection bit.

Figure 4-1. Coding of the PARAM byte in the REQB/WUPB command.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	RW	N		

Table 4-4. Coding of “N”, the number of anticollision slots, in the PARAM byte.

Bit 2	Bit 1	Bit 0	N
0	0	0	1
0	0	1	2
0	1	0	4
0	1	1	8
1	0	0	16
1	0	1	RFU
1	1	x	RFU

Table 4-5. Coding of the REQB / WUPB selection bit in the PARAM byte.

Bit 3	Command
0	REQB
1	WUPB

CRC: Communication error detection bytes.

4.2.3 Response Field Descriptions

PUPI: PseudoUnique PICC Identifier. This is the card ID used for anticollision, stored in the System Zone.

APP: Application Data. Information about the card or application, stored in the System Zone.

The fourth byte of the application data field, APP3, is programmed by Atmel with a memory density code at the factory to permit easy identification of different card sizes. The memory density codes programmed by Atmel are shown in Table 4-6.

Table 4-6. Default value of APP3 is the CryptoRF Memory Density Code

Device Number	Density Code
AT88SC0104CRF	$02
AT88SC0204CRF	$12
AT88SC0404CRF	$22
AT88SC0808CRF	$33
AT88SC1616CRF	$44
AT88SC3216CRF	$54
AT88SC6416CRF	$64

Protocol: ISO/IEC 14443 communication capabilities reported to the PCD.

CRC: Communication error detection bytes.

4.2.4 Error Handling

If an REQB or WUPB command containing errors is received by the PICC, it is ignored and no response is send.

4.3 Slot MARKER Command [$s5]

The Slot MARKER command can be used to separately identify multiple PICCs in the RF field. The command and response are ISO/IEC 14443-3:2001 compliant..

	Reader	PICC

Command >

"S"	$5
CRC1	
CRC2	

ATQB Response >

$50	SUCCESS RESPONSE
PUPI 0	System Zone Byte $00
PUPI 1	System Zone Byte $01
PUPI 2	System Zone Byte $02
PUPI 3	System Zone Byte $03
APP 0	System Zone Byte $04
APP 1	System Zone Byte $05
APP 2	System Zone Byte $06
APP 3	System Zone Byte $07
Protocol 1	$00
Protocol 2	System Zone Byte $08
Protocol 3	$51
CRC1	
CRC2	

4.3.1 Operation

Slot MARKER is an optional command used to perform ISO/IEC 14443-3 Type B anticollision using the timeslot approach. Immediately after an REQB or WUPB command with "N" greater than 1 is issued, and the ATQB response (if any) is received, the PCD will transmit Slot MARKER commands with slot values "S" of 2 to "N" to define the start of each timeslot for anti-collision. If the random number "R" selected by the PICC matches "S" then the PICC responds with ATQB. PICCs in the Active State are not permitted to answer this command.

4.3.2 Command Field Descriptions

S: The slot number "S" is encoded within the command byte as shown in Table 4-7.

CRC: Communication error detection bytes.

4.3.3 Response Field Descriptions

Table 4-7. Coding of the slot number within the Slot MARKER command byte.

Bit 7	Bit 6	Bit 5	Bit 4	Slot
0	0	0	0	*Not Supported*
0	0	0	1	2
0	0	1	0	3
0	0	1	1	4
0	1	0	0	5
0	1	0	1	6
0	1	1	0	7
0	1	1	1	8
1	0	0	0	9
1	0	0	1	10
1	0	1	0	11
1	0	1	1	12
1	1	0	0	13
1	1	0	1	14
1	1	1	0	15
1	1	1	1	16

PUPI: PseudoUnique PICC Identifier. This is the card ID used for anticollision, stored in the System Zone.

APP: Application Data. Information about the card or application, stored in the System Zone.

Protocol: ISO/IEC 14443 communication capabilities reported to the PCD.

CRC: Communication error detection bytes.

4.3.4 Error Handling

If a Slot MARKER command containing errors is received by the PICC, it is ignored and no response is send.

4.4 ATTRIB Command [$1D]

The ATTRIB command is used to select a PICC for a transaction. The command and response are ISO/IEC 14443-3:2001 compliant.

	Reader	PICC
Command >	$1D	
	PUPI 0	
PUPI of PCI >	PUPI 1	
	PUPI 2	
	PUPI 3	
Param 1 >	$00	
Param 2 >	$0 / TBmax	
Param 3 >	$00	
Param 4 Assigns CID >	$0 / CID	
	CRC1	
	CRC2	

ATTRIB Response >	$0 / CID		SUCCESS RESPONSE
	CRC1		
	CRC2		

4.4.1 Operation

Sending the ATTRIB command (with a matching PUPI) after an ATQB response places the PICC in the Active State and assigns the Card ID Number (CID) to the PICC. PICCs already in the Active State or Halt State are not permitted to answer this command.

4.4.2 Command Field Descriptions

PUPI: PseudoUnique PICC Identifier. This is the card ID used for anticollision, stored in the System Zone.

Param: ISO/IEC 14443 communication capabilities reported to the PICC. The contents of Param Bytes 1, 2, and 3 are not used by the CryptoRF family.

TBmax: A parameter sent by the PCD reporting the receive buffer size of the PCD. Default value is $0.

CID: The Card ID Number (CID) in ATTRIB Param Byte 4 and in the ATTRIB Response is encoded as shown in Table 4-8. Each PICC is assigned a unique CID when it is placed in the Active State. CryptoRF Active State commands use the assigned CID to direct the commands to the desired PICC.

Table 4-8. Coding of the Card ID in the ATTRIB command and response.

Bit 7	Bit 6	Bit 5	Bit 4	CID
0	0	0	0	*Not Supported*
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7
1	0	0	0	8
1	0	0	1	9
1	0	1	0	10
1	0	1	1	11
1	1	0	0	12
1	1	1	1	13
1	1	1	0	14
1	1	1	1	*Not Supported*

CRC: Communication error detection bytes.

4.4.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

CRC: Communication error detection bytes.

4.4.4 Error Handling

If an ATTRIB command containing transmission errors is received by the PICC, it is ignored and no response is send.

4.5 HLTB Command [$50]

The HLTB command places a PICC in the Halt State, where it is not allowed to answer an REQB command. The command and response are ISO/IEC 14443-3 compliant.

	Reader	PICC
Command >	$50	
	PUPI 0	
PUPI of PCI >	PUPI 1	
	PUPI 2	
	PUPI 3	
	CRC1	
	CRC2	
HLTB Response >		$00 SUCCESS RESPONSE
		CRC1
		CRC2

4.5.1 Operation

Sending the “Halt B” (HLTB) command (with a matching PUPI) after an ATQB response places the PICC in the Halt State. A PICC in the Halt State will only respond to a WUPB command. PICCs in the Active State or already in the Halt State are not permitted to answer this command.

4.5.2 Command Field Descriptions

PUPI: PseudoUnique PICC Identifier. This is the card ID used for anticollision, stored in the System Zone.

CRC: Communication error detection bytes.

4.5.3 Response Field Descriptions

CRC: Communication error detection bytes.

4.5.4 Error Handling

If a HLTB command containing errors is received by the PICC, it is ignored and no response is send.

4.6 Active State Command Definitions

Commands in this section are arranged in order by the hexadecimal code in the command byte.

Table 4-9. Coding of the Command byte for the CryptoRF Active State Command Set

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Command Name	Hexidecimal
CID				0	0	0	1	Set User Zone	$c1
CID				0	0	1	0	Read User Zone	$c2
CID				0	0	1	1	Write User Zone	$c3
CID				0	1	0	0	Write System Zone	$c4
CID				0	1	1	0	Read System Zone	$c6
CID				1	0	0	0	Verify Crypto	$c8
CID				1	0	0	1	Send Checksum	$c9
CID				1	0	1	0	DESELECT	$cA
CID				1	0	1	1	IDLE	$cB
CID				1	1	0	0	Check Password	$cC
All Other Values are Not Supported									

4.6.1 Response Format

The response to each Active State command consists of five bytes or more. The first byte of the response is the command byte echoed back to the PCD. The second byte is the ACK/NACK byte which reports success or failure of the command execution. The final two bytes of the response are always the CRC bytes. The CRC bytes are preceded by a STATUS byte which reports error codes or PICC status codes. Any data bytes returned by the command are located between the ACK/NACK and STATUS bytes.

Table 4-10. Coding of the ACK/NACK byte of the PICC response

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Response Decode
0	0	0	0	0	0	0	0	ACK
0	0	0	0	0	0	0	1	NACK, See STATUS byte for cause
Password Attempts Counter				0	0	0	1	NACK, Check Password Attempt Failure
Auth. Attempts Counter				0	0	0	1	NACK, Authentication or Encryption Attempt Failure

The STATUS byte reports reasons for failure of an operation, and provides feedback to the host application indicating status of the PICC. The PICC ignores commands that do not have a matching CID. Invalid command codes are also ignored.

4.7 Set User Zone Command [$c1]

The Set User Zone command selects the user memory area to be addressed by the Read User Zone and Write User Zone commands.

	Reader	PICC
Command >	CID | $1 PARAM CRC1 CRC2	
Echo Command >		CID | $1 ACK/NACK STATUS CRC1 CRC2

4.7.1 Operation

Before reading and writing data to the user memory, the host must select a User Zone with this command. Only one User Zone may be selected at a time. At the time the zone is selected the host also chooses whether anti-tearing should be active for this zone. If anti-tearing is activated, then all writes to the User Zone will utilize anti-tearing until a new Set User Zone command is received. Only PICCs in the Active State are permitted to answer this command.

4.7.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

PARAM: Selects the User Zone and sets anti-tearing on or off. When the anti-tearing bit (bit 7) is set to 1b then anti-tearing is enabled, when set to 0b normal writes are selected.

Figure 4-2. Coding of the PARAM byte of the Set User Zone command

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
AT	0	0	0	User Zone			

Table 4-11. Coding of the User Zone number within the PARAM byte

Bit 3	Bit 2	Bit 1	Bit 0	User Zone
0	0	0	0	0
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7
1	0	0	0	8
1	0	0	1	9
1	0	1	0	10
1	0	1	1	11
1	1	0	0	12
1	1	0	1	13
1	1	1	0	14
1	1	1	1	15

CRC: Communication error detection bytes.

4.7.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.7.4 Error Handling

If a Set User Zone command containing transmission errors is received by the PICC, it is ignored and no response is send.

Table 4-12. Status Codes returned in the Set User Zone response

Error/Status Message	Status Code	Type
No Errors	$00	ACK
User Zone PARAM Invalid	$A1	NACK

4.8 Read User Zone Command [$c2]

The Read User Zone command reads data from the currently selected User Zone. See Read User Zone (Large Memory) command for the AT88SC6416CRF read command information.

	Reader	PICC	
Command >	CID	$2	
	$00		
	ADDR		
	“L”		
	CRC1		
	CRC2		
Echo Command >	CID	$2	FAILURE RESPONSE
	NACK		
	STATUS		< Error Code
	CRC1		
	CRC2		
Echo Command >	CID	$2	SUCCESS RESPONSE
	ACK		
	DATA 1		
	DATA 2		
	.....		
	DATA “L”		
	DATA “L+1”		
	STATUS		< Status Code
	CRC1		
	CRC2		

4.8.1 Operation

The Read User Zone command reads data from the device's currently selected User Zone.

The data byte address is internally incremented as each byte is read from memory. If the data byte address increments beyond the end of the current zone during a read, then the address will "roll over" to the first byte of the same zone. Only PICCs in the Active State are permitted to answer this command.

4.8.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

ADDR: The starting address of the data to read.

L: The number of bytes to read minus 1. L cannot exceed the size of the user zone.

Reading more than 64 bytes in a single operation is not recommended. In a typical application environment, optimal transaction time is achieved by reading no more than 32 data bytes in a single operation.

CRC: Communication error detection bytes.

4.8.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

DATA: The data bytes read from user memory.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.8.4 Error Handling

If a Read User Zone command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

Table 4-13. Status Codes returned in the Read User Zone response

Error/Status Message	Status Code	Type
No errors	$00	ACK
Access Denied (User Zone Not Set)	$99	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Authentication or Encryption Activation Required	$A9	NACK
Password Required	$D9	NACK
Memory Access Error	$EE	ACK/NACK

4.9 Read User Zone (Large Memory) Command [$c2]

The Read User Zone (Large Memory) command reads data from the currently selected User Zone. This command format applies to the AT88SC6416CRF device only.

	Reader	PICC	
Command >	CID | $2		
	ADDR H		
	ADDR L		
	"L"		
	CRC1		
	CRC2		
Echo Command >		CID | $2	FAILURE RESPONSE
		NACK	
		STATUS	< Error Code
		CRC1	
		CRC2	
Echo Command >		CID | $2	SUCCESS RESPONSE
		ACK	
		DATA 1	
		DATA 2	
		.....	
		DATA "L"	
		DATA "L+1"	
		STATUS	< Status Code
		CRC1	
		CRC2	

4.9.1 Operation

The Read User Zone (Large Memory) command operates identically to the standard Read User Zone command, but utilizes a two byte address to support large memory sizes. The Read User Zone command reads data from the device's currently selected User Zone. The data byte address is internally incremented as each byte is read from memory. If the data byte address increments beyond the end of the current zone during a read, then the address will "roll over" to the first byte of the same zone. Only PICCs in the Active State are permitted to answer this command.

4.9.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

ADDR: The two byte starting address of the location to be written.

Figure 4-3. Format of the ADDR H byte of the Write User Zone (Large Memory) command

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	A8

L: The number of bytes to read minus 1. L cannot exceed the size of the user zone.

Reading more than 64 bytes in a single operation is not recommended. In a typical application environment, optimal transaction time is achieved by reading no more than 32 data bytes in a single operation.

CRC: Communication error detection bytes.

4.9.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

DATA: The data bytes read from user memory.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.9.4 Error Handling

If a Read User Zone command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

Table 4-14. Status Codes returned in the Read User Zone (Large Memory) response.

Error/Status Message	Status Code	Type
No Errors	$00	ACK
Access Denied (User Zone Not Set)	$99	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Authentication or Encryption Activation Required	$A9	NACK
Password Required	$D9	NACK
Memory Access Error	$EE	ACK/NACK

4.10 Write User Zone Command [$c3]

The Write User Zone command writes data into the currently selected User Zone. See Write User Zone (Large Memory) command for the AT88SC6416CRF write command information.

	Reader	PICC

Command >

CID	$3
$00	
ADDR	
“L”	
DATA 1	
DATA 2	
.....	
DATA “L”	
DATA “L+1”	
CRC1	
CRC2	

Echo Command >

CID	$3
ACK/NACK	
STATUS	
CRC1	
CRC2	

4.10.1 Operation

The Write User Zone command writes data in the device's currently selected User Zone. As each byte is clocked in to the memory the lower bits of the address are internally incremented. The upper address bits are not incremented, so the page address remains constant.

Write operations cannot cross page boundaries; a Write User Zone command can only write data bytes within a single physical memory page. Attempts to write beyond the end of the page boundary will wrap to the beginning of the same page. Only PICCs in the Active State are permitted to answer this command.

4.10.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

ADDR: The starting address of the location to be written.

L: The number of bytes to read minus 1. “L” cannot exceed the physical page size of the memory. In anti-tearing mode the maximum number of bytes that can be written is 8 bytes. If the

Access Register enables Write Lock mode or Program Only mode, the maximum number of bytes that can be written is 1 byte.

Table 4-15. Write Characteristics of CryptoRF

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88SC0104CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC0204CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC0404CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC0808CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC1616CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC3216CRF	1 to 32 Bytes	1 to 8 Bytes

DATA: The data bytes to be written into user memory.

CRC: Communication error detection bytes.

4.10.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.10.4 Error Handling

If a Write User Zone command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

Table 4-16. Status Codes returned in the Write User Zone response

Error/Status Message	Status Code	Type
No Errors	$00	ACK
Write Pending - Checksum Required	$0C	ACK
One Byte Written (Write Lock Mode)	$1B	ACK
Access Denied (User Zone Not Set)	$99	NACK
Access Denied (Security Fuses Invalid)	$99	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Authentication or Encryption Activation Required	$A9	NACK
Data Written (Program Only Mode)	$B0	ACK
Access Denied (Write Lock Mode)	$B9	NACK
Password Required	$D9	NACK
Modify Forbidden	$E9	NACK
Memory Access Error	$EE	ACK/NACK

4.11 Write User Zone (Large Memory) Command [$c3]

The Write User Zone command writes data into the currently selected User Zone. This command format applies to the AT88SC6416CRF device only.

Reader	PICC

Command >

CID	$3
ADDR H	
ADDR L	
“L”	
DATA 1	
DATA 2	
.....	
DATA “L”	
DATA “L+1”	
CRC1	
CRC2	

Echo Command >

CID	$3
ACK/NACK	
STATUS	
CRC1	
CRC2	

4.11.1 Operation

The Write User Zone (Large Memory) command operates identically to the standard Write User Zone command, but utilizes a two byte address to support large memory sizes. The Write User Zone command writes data in the device's currently selected User Zone. As each byte is clocked in to the memory the lower bits of the address are internally incremented. The upper address bits are not incremented, so the page address remains constant.

Write operations cannot cross page boundaries; a Write User Zone command can only write data bytes within a single physical memory page. Attempts to write beyond the end of the page boundary will wrap to the beginning of the same page. Only PICCs in the Active State are permitted to answer this command.

4.11.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

ADDR: The two byte starting address of the location to be written.

Figure 4-4. Format of the ADDR H byte of the Write User Zone (Large Memory) command

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	A8

L: The number of bytes to read minus 1. “L” cannot exceed the physical page size of the memory. In anti-tearing mode the maximum number of bytes that can be written is 8 bytes. If the Access Register enables Write Lock mode or Program Only mode, the maximum number of bytes that can be written is 1 byte.

Table 4-17. Write Characteristics of Large Memory CryptoRF

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88SC6416CRF	1 to 32 Bytes	1 to 8 Bytes

DATA: The data bytes to be written into user memory.

CRC: Communication error detection bytes.

4.11.3 Response Field Descriptions

CID: The PICC transmits it’s assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.11.4 Error Handling

If a Write User Zone command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

Table 4-18. Status Codes returned in the Write User Zone (Large Memory) response

Error/Status Message	Status Code	Type
No Errors	$00	ACK
Write Pending - Checksum Required	$0C	ACK
One Byte Written (Write Lock Mode)	$1B	ACK
Access Denied (User Zone Not Set)	$99	NACK
Access Denied (Security Fuses Invalid)	$99	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Authentication or Encryption Activation Required	$A9	NACK
Data Written (Program Only Mode)	$B0	ACK
Access Denied (Write Lock Mode)	$B9	NACK
Password Required	$D9	NACK
Modify Forbidden	$E9	NACK
Memory Access Error	$EE	ACK/NACK

4.12 Write System Zone Command [$c4]

The Write System Zone command writes data to the configuration memory. This command is also used to program the security fuses.

Reader	PICC

Command >

CID	$4
PARAM	
ADDR	
“L”	
DATA 1	
DATA 2	
.....	
DATA “L”	
DATA “L+1”	
CRC1	
CRC2	

Echo Command >

CID	$4
ACK/NACK	
STATUS	
CRC1	
CRC2	

4.12.1 Operation

The Write System Zone command writes data into the configuration memory. As each byte is clocked in to the memory the lower bits of the address are internally incremented. The upper address bits are not incremented, so the page address remains constant.

Write operations cannot cross page boundaries; a Write System Zone command can only write data bytes within a single physical memory page. Attempts to write beyond the end of the page boundary will wrap to the beginning of the same page. Only PICCs in the Active State are permitted to answer this command.

A special mode of the Write System Zone programs the security fuses. Once programmed, the fuses cannot be erased.

4.12.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte selects the type of write operation to be performed.

Table 4-19. PARAM byte options for the Write System Zone command

Command	PARAM	ADDR	"L"	DATA
Write System Zone	$00	address	# of bytes - 1	"L+1" bytes
Write System Zone w/ AT	$80	address	# of bytes - 1	"L+1 bytes"
Write Fuse Byte	$01	fuse addr	$00	1 bytes
All Other Values Are Not Supported				

Table 4-20. Coding of ADDR for Fuse Programming Only

Hex	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Fuse
$07	0	0	0	0	0	1	1	1	SEC
$06	0	0	0	0	0	1	1	0	FAB
$04	0	0	0	0	0	1	0	0	CMA
$00	0	0	0	0	0	0	0	0	PER

ADDR: The starting address of the data to write. When performing a fuse byte write the ADDR byte contains the address of the fuse; only one fuse may be programmed per Write System Zone command.

L: The number of bytes to read minus 1. L cannot exceed the physical page size of the memory. In anti-tearing mode the maximum number of bytes that can be written is 8 bytes. If the Access Register enables Write Lock Mode or Program Only Mode, the maximum number of bytes that can be written is 1 byte.

Table 4-21. Write Characteristics of CryptoRF configuration memory

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88SC0104CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC0204CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC0404CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC0808CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC1616CRF	1 to 16 Bytes	1 to 8 Bytes
AT88SC3216CRF	1 to 32 Bytes	1 to 8 Bytes
AT88SC6416CRF	1 to 32 Bytes	1 to 8 Bytes

DATA: The data bytes to be written into configuration memory.

One byte of data is required to be sent when writing the fuse byte, however the contents of this byte are ignored.

CRC: Communication error detection bytes.

4.12.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.12.4 Error Handling

If a Write System Zone command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

.

Table 4-22. Status Codes returned in the Write System Zone response

Error/Status Message	Status Code	Type
No Errors	$00	ACK
PARAM Invalid	$A1	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Access Denied (Write Not Allowed)	$BA	NACK
Memory Access Error	$EE	ACK/NACK

.

Table 4-23. Status Codes returned in the Write System Zone response for Fuse Writes

Error/Status Message	Status Code	Type
Fuse Byte (Successful Fuse Byte Write)	fuse byte	ACK
Fuse Address Invalid	$A2	NACK
Password Required	$D9	NACK
Fuse Access Denied	$DF	NACK
Access Denied (Fuse Order Incorrect)	$E9	NACK
Memory Access Error	$EE	ACK/NACK

4.13 Read System Zone Command [$c6]

The System Read command allows reading of system data from the configuration memory, from the security fuses, or from the checksum register.

Reader	PICC

Command >

CID	$6
PARAM	
ADDR	
“L”	
CRC1	
CRC2	

Echo Command >

CID	$6	FAILURE RESPONSE
NACK		
STATUS		< Error Code
CRC1		
CRC2		

Echo Command >

CID	$6	SUCCESS RESPONSE
ACK		
DATA 1		
DATA 2		
.....		
DATA “L”		
DATA “L+1”		
STATUS		< Status Code
CRC1		
CRC2		

4.13.1 Operation

The Read System Zone command reads from the devices configuration memory. The data byte address is internally incremented as each byte is read from the memory. If the data byte address increments into a segment where read access is forbidden, the “fuse byte” is transmitted in place of the forbidden data.

Depending on the value of the PARAM byte, the host may read the data in the configuration memory, the fuses, or a checksum. Only PICCs in the Active State are permitted to answer this command.

4.13.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte selects the type of read operation to be performed.

Table 4-24. PARAM byte options for the Read System Zone command

Command	PARAM	ADDR	"L"
Read System Zone	$00	address	# of bytes - 1
Read Fuse Byte	$01	$FF	$00
Read Checksum	$02	$FF	$01
All Other Values Are Not Supported			

ADDR: The starting address of the data to read.

L: The number of bytes to read minus 1. L cannot exceed 240 bytes.

Reading more than 64 bytes in a single operation is not recommended. In a typical application environment, optimal transaction time is achieved by reading no more than 32 bytes in a single operation.

CRC: Communication error detection bytes.

4.13.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

DATA: The data bytes read from the configuration memory.

Since access rights vary throughout the system zone, the host may provide an authorized starting address, but a length that causes the device to reach forbidden data. In this case, the device will transmit the authorized bytes, but unauthorized bytes will be replaced by the "fuse byte". An "Access Denied" status code $BA or $BC will be returned to indicate that some of the bytes returned were replaced by the "fuse byte".

Figure 4-5. Coding of the data byte received when reading the fuse byte

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

When the Read Fuse Byte option is activated, only a single data byte is returned. When the Read Checksum option is activated, two bytes are returned.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.13.4 Error Handling

If a Read System Zone command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response..

Table 4-25. Status Codes returned in the Read System Zone response

Error/Status Message	Status Code	Type
No Errors	$00	ACK
PARAM Invalid	$A1	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Byte Access Denied (Read Not Allowed)	$BA	ACK/NACK
Byte Access Denied (Password Required)	$BC	ACK/NACK
Memory Access Error	$EE	ACK/NACK

4.14 Verify Crypto Command [$c8]

The Verify Crypto command is used in the Authentication mode and the Encryption mode only. See the document *CryptoRF Specification Addendum for Secure Applications* for information.

4.15 Send Checksum Command [$c9]

The Send Checksum command is used in the Authentication mode and the Encryption mode only. See the document *CryptoRF Specification Addendum for Secure Applications* for information.

4.16 DESELECT Command [$cA]

The DESELECT command places a PICC in the Halt State.

Reader	PICC

Command >

CID	$A
CRC1	
CRC2	

Echo Command >

CID	$A
ACK	
STATUS	
CRC1	
CRC2	

4.16.1 Operation

Sending the DESELECT command (with a matching CID) to a PICC in the Active State places the PICC in the Halt State. The User Zone, password, and authentication registers are cleared before the PICC enters the Halt State. Only PICCs in the Active State are permitted to answer this command.

4.16.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

CRC: Communication error detection bytes.

4.16.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.16.4 Error Handling

If a DESELECT command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

Table 4-26. Status Codes returned in the DESELECT response

Error/Status Message	Status Code	Type
No errors	$00	ACK

4.17 IDLE Command [$cB]

The IDLE command resets the PICC and places it in the Idle State.

Reader	PICC

Command >

CID	$B
CRC1	
CRC2	

Echo Command >

CID	$B
ACK	
STATUS	
CRC1	
CRC2	

4.17.1 Operation

Sending the IDLE command (with a matching CID) to a PICC in the Active State resets the PICC and places it in the Idle State. The User Zone, password, and authentication registers are cleared before the PICC enters the Idle State. The PICC responds only to successful IDLE commands. Only PICCs in the Active State are permitted to answer this command.

4.17.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

CRC: Communication error detection bytes.

4.17.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.17.4 Error Handling

If an IDLE command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response.

Table 4-27. Status Codes returned in the IDLE response

Error/Status Message	Status Code	Type
No errors	$00	ACK

4.18 Check Password Command [$cC]

The Check Password command transmits a password for validation.

Reader	PICC

Command >

CID	$C
Password Index	
PW 1	
PW 2	
PW 3	
CRC1	
CRC2	

Echo Command >

CID	$C
ACK/NACK	
STATUS	
CRC1	
CRC2	

4.18.1 Operation

To read or write data in User Zones that require a password for access the host must carry out a password validation operation. The host uses the Check Password command to send the password for validation against the password selected with the Password Index byte. Only PICCs in the Active State are permitted to answer this command.

If the Check Password is successful, the Password Attempts Counter (PAC) is cleared and the ACK response is issued. Only one password is active at any time. If the Check Password fails, the PAC is incremented and a NACK response is issued. The Check Password success or failure is memorized and active until the PICC is powered down, removed from the Active state, or until a new Check Password is received. If the password trials limit is reached, subsequent Check Password commands will be rejected.

4.18.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

Password Index: Identifies the password register that the PICC will check the transmitted password against.

Table 4-28. Coding of the Password Index for 1K, 2K, and 4K bit CryptoRF devices

Password Index	Check Password
$10	Password Read 0
$11	Password Read 1
$12	Password Read 2
$17	Password Read 7
$00	Password Write 0
$01	Password Write 1
$02	Password Write 2
$07	Password Write 7
All Other Values Are Not Supported	

.

Table 4-29. Coding of the Password Index for 8K bit and larger CryptoRF devices

Password Index	Check Password
$10	Password Read 0
$11	Password Read 1
$12	Password Read 2
$13	Password Read 3
$14	Password Read 4
$15	Password Read 5
$16	Password Read 6
$17	Password Read 7
$00	Password Write 0
$01	Password Write 1
$02	Password Write 2
$03	Password Write 3
$04	Password Write 4
$05	Password Write 5
$06	Password Write 6
$07	Password Write 7
All Other Values Are Not Supported	

PW: The password bytes.

CRC: Communication error detection bytes.

4.18.3 Response Field Descriptions

CID: The PICC transmits it's assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

NACK: Not Acknowledge, the command did not execute correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

4.18.4 Error Handling

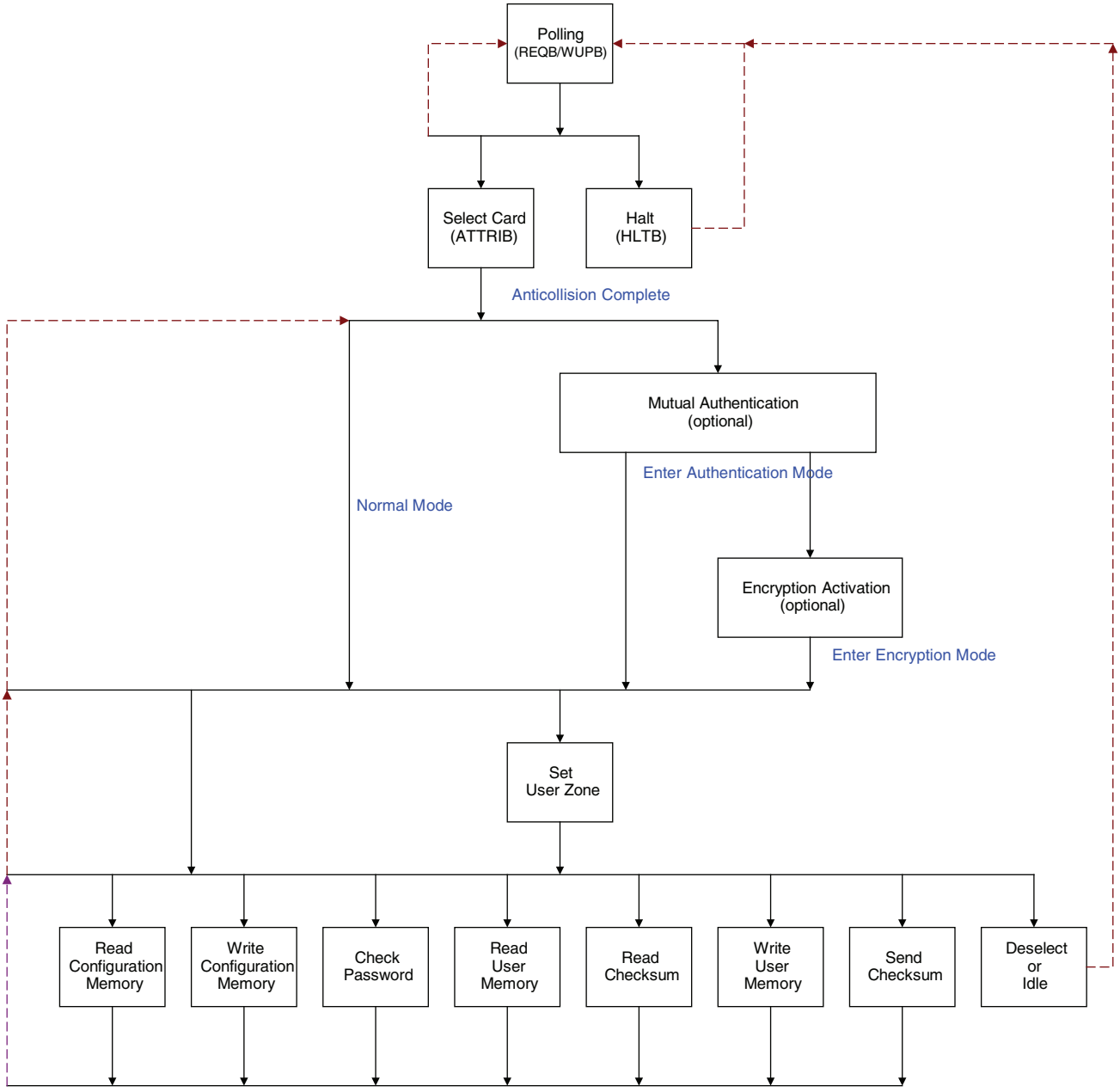
If a Check Password command containing transmission errors is received by the PICC, it is ignored and no response is send. The PICC reports errors in the status byte of the response..

Table 4-30. Status Codes returned in the Check Password response

Error/Status Message	Status Code	Type
No errors	$00	ACK
Password Index Invalid	$A1	NACK
Check Password Failure	$D9	NACK
Memory Access Error (Security Operation)	$F9	NACK
Memory Access Error	$EE	ACK/NACK

5. Transaction Flow

Figure 5-1. Flowchart of a Typical CryptoRF Transaction



In a typical CryptoRF transaction the host performs anticollision, selects a User Zone, and reads or writes the user memory. When a User Zone requires a password, authentication, or encryption the host performs the required security operation before accessing the User Zone. Note that the Set User Zone command may be sent before or after the security operation.

6. Absolute Maximum Ratings*

* 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 may affect device reliability.

Absolute Maximum Rating	
Operating Temperature (junction)	-40°C to +85°C
Storage Temperature (ambient)	-65°C to +150°C
HBM ESD (Antenna Pins only)	2000V minimum

The maximum temperature ratings in this section are applicable to CryptoRF in wafer form. When assembled into a package the CryptoRF temperature ratings may be reduced to reflect the limitations of the package. However the CryptoRF absolute maximum ratings should not be exceeded for any package.

7. Reliability

Parameter	Min	Typ	Max	Units
Write Endurance (each Byte)	100,000			Write Cycles
Anti-Tearing Write Endurance	50,000			Writes
Data Retention (at 55°C)	10			Years
Data Retention (At 35°C)	30	50		Years
Read Endurance	Unlimited			Read Cycles

CryptoRF is fabricated with Atmel’s high reliability CMOS EEPROM manufacturing technology. The write endurance and data retention EEPROM reliability ratings apply to each byte of the user and configuration memory.

The optional CryptoRF anti-tearing functions use a single anti-tearing EEPROM buffer memory. Every anti-tearing write operation utilizes the same buffer. The anti-tearing write endurance specification is a limitation in the total number of anti-tearing write operations that can be performed by each die.

8. Electrical Characteristics

Symbol	Parameter	Min	Normal	Max	Units
C_r	Integrated Tuning Capacitance	72	82	92	pF
T_{POR}	Polling Reset Time (no anti-tearing to process)			5	mS
T_{POR-AT}	Polling Reset Time (anti-tearing write to process)			10	mS
T_{WR}	Write Cycle Time of EEPROM Memory		1.6	2.0	mS

8.1 Tamper Detection

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

Annex A: Terms and Abbreviations

A	Unmodulated PCD field amplitude. Used in modulation index calculation.
A/m	Amperes per Meter. Units of magnetic field strength
AC	Alternating Current.
ACK	Acknowledge response, indicates success of the requested operation.
Active state	The state of a PICC that is selected and ready to receive commands.
ADDR	Address identifying the location to begin a read or write operation.
AFI	Application Family Identifier. Used during Type B anticollision.
APP	Application bytes.
AR	Access Register.
ASK	Amplitude Shift Keying modulation. PCD data transmission signaling format.
AT	Anti-tearing.
ATQB	Answer to Request Type B. The response to a polling command.
ATTRIB	PICC Selection Command, Type B.
B	Modulated PCD field amplitude. Used in modulation index calculation.
Card	A PICC with loop antenna in a plastic card or other RFID form.
CID	Card ID. The 4 bit code used to identify a PICC in the Active state.
CMA	The third of four security fuses.
CRC	Cyclic Redundancy Check = 16 bit RF Communication Error Detection Code.
CRC_B	Cyclic Redundancy Check, Type B.
CRF	CryptoRF
C_T	Tuning Capacitance. The capacitance between antenna pins AC1 and AC2.
DATA	Bytes for EEPROM memory read or write.
DCR	Device Configuration Register. Address $18 in the Configuration Memory.
EEPROM	Nonvolatile memory.
EGT	Extra Guard Time.
EGTL	Extra Guard Time Length. A DCR mode control bit.
EOF	End of Frame.
ETA	Extended Trials Allowed. A DCR mode control bit.
ETU	Elementary Time Unit = 128 carrier cycles (9.4395 uS nominal).
FAB	The second of four security fuses.
fc	Carrier Frequency = 13.56 MHz nominal.
Fo	Resonant Frequency.
FO	Frame Option.
fs	Subcarrier Frequency = fc/16 = 847.5 kHz nominal.
FWI	Frame Waiting Time Integer. Protocol bits communicating the PICC FWT time.

FWT	Frame Waiting Time. Maximum time the PCD must wait for a PICC response.
Halt state	The state of a PICC waiting for a WUPB command (ignoring all other commands).
HLTB	Halt command, Type B.
Hmin	Minimum unmodulated operating magnetic field strength.
Hmax	Maximum unmodulated operating magnetic field strength.
Host	The RF reader, firmware, and application software communicating with the PICC.
i	Variable for the Index of a Password Set or Key Set.
IC	Integrated Circuit.
ID	Identification.
Idle state	The state of a PICC after power on reset, waiting for a REQB or WUPB command.
IEC	International Electrotechnical Commission. www.iec.ch
ISO	International Organization for Standardization. www.iso.org
J	Loop Count Variable in a Flowchart.
kbps	KiloBits Per Second.
kHz	KiloHertz.
L	Variable for the Length code in a CryptoRF read or write command. L = (N-1)
LSB	Least Significant Bit.
MDF	Modify Forbidden. Access Register mode control bit.
M.D.	PCD Modulation Depth.
MHz	MegaHertz.
M.I.	PCD Modulation Index. Calculated from calibration coil voltages as (A – B)/(A + B)
mm	MilliMeter.
mS	MilliSecond.
uS	MicroSecond
MSB	Most Significant Bit.
MTZ	Memory Test Zone. Address $0A and $0B in the Configuration Memory.
mV	MilliVolt.
N	Variable for the Number of anticollision slots.
N	Variable for the Number of bytes in a read or write command. N = (L+1)
NACK	Not Acknowledge Response, Indicates failure of the requested operation
NRZ-L	Non-Return to Zero (L for Level) data encoding. PICC data transmission coding.
nS	NanoSecond.
OTP	One Time Programmable. Memory that cannot be erased or rewritten.
PAC	Password Attempts Counter.
PARAM	A byte containing option codes or variables.
PCD	Proximity Coupling Device. The RF reader/writer and antenna.
PER	The fourth of four security fuses.

PGO	Program Only mode. Access Register mode control bit.
PICC	Proximity Integrated Circuit Card. The card/tag containing the IC and antenna.
PM	Password Mode. Access Register mode control bit.
PR	Password Register.
Protocol	Bytes communicating ISO protocol information.
PUPI	Pseudo Unique PICC Identifier. ID for anticollision.
PW	Password.
R	Random number selected by PICC during anticollision.
RBmax	Receive Buffer size code. ATQB protocol byte returned by PICC.
RF	Radio Frequency.
RFU	Reserved for Future Use. Any feature or bit reserved by ISO or by Atmel.
rms	Root Mean Square.
ROM	Read Only Memory.
RW	REQB/WUPB command selection code.
S	Slot Number. A code sent to the PICC with Slot MARKER command.
SEC	The first of four security fuses.
SME	Supervisor Mode Enable. A DCR mode control bit.
STATUS	A response byte containing information on the status of the PICC.
Tag	A PICC with loop antenna attached in a non-plastic credit card form.
TBmax	An ISO/IEC 14443-3 protocol code indicating the receive buffer size of the PCD.
T_{POR}	Polling Response Time.
T_{POR-AT}	Polling Response Time with Anti-Tearing.
TR0	Guard Time per ISO/IEC 14443-2.
TR1	Synchronization Time per ISO/IEC 14443-2.
TR2	PICC to PCD frame delay time (per ISO/IEC 14443-3 Amendment 1).
T_{WR}	EEPROM Write Cycle Time.
UZ	User Zone.
WG8	ISO/IEC Working Group eight. Develops standards for contactless smartcards.
WLM	Write Lock Mode. Access Register mode control bit.
WUPB	Wake Up command, Type B.
z	Variable for the Index of a Password Set or Key Set.

Annex B: Standards and Reference Documents

B.1 International Standards

CryptoRF is designed to comply with the requirements of the following ISO/IEC standards for Type B PICCs operating at the standard 106 kbps data rate.

ISO/IEC 7810:1995 *Identification Cards – Physical Characteristics*

ISO/IEC 10373-6:2001 *Identification Cards – Test Methods – Part 6: Proximity Cards*

ISO/IEC 14443-1:2000 *Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 1: Physical Characteristics*

ISO/IEC 14443-2:2001 *Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 2: Radio Frequency Power and Signal Interface*

ISO/IEC 14443-3:2001 *Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 3: Initialization and Anticollision*

ISO/IEC standards are available at www.ansi.org, www.iso.org, and from your national standards organization. The ISO/IEC 14443 and ISO/IEC 10373 standards were developed by the WG8 committee (www.wg8.de).

B.2 References

Atmel Application Note: *Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards.* Document 2056x (Available at www.atmel.com)

CryptoRF Ordering Codes: *CryptoRF and Secure RF Standard Product Offerings.* Document 5047x (Available at www.atmel .com)

Annex C: User Memory Maps

CryptoRF User Memory is divided into equal size User Zones as summarized in Table C-1. Access requirements for each zone are independently configured by the customer using the Access Control Registers. See Annex G for more information on access control.

Table C-1. CryptoRF User Memory Characteristics

CryptoRF Part Number	User Memory Size		User Memory Organization		Write Characteristics	
	Bits	Bytes	# Zones	Bytes / Zone	Standard Write	Anti-Tearing Write
AT88SC0104CRF	1K	128	4	32	1 to 16 Bytes	1 to 8 Bytes
AT88SC0204CRF	2K	256	4	64	1 to 16 Bytes	1 to 8 Bytes
AT88SC0404CRF	4K	512	4	128	1 to 16 Bytes	1 to 8 Bytes
AT88SC0808CRF	8K	1K	8	128	1 to 16 Bytes	1 to 8 Bytes
AT88SC1616CRF	16K	2K	16	128	1 to 16 Bytes	1 to 8 Bytes
AT88SC3216CRF	32K	4K	16	256	1 to 32 Bytes	1 to 8 Bytes
AT88SC6416CRF	64K	8K	16	512	1 to 32 Bytes	1 to 8 Bytes

Note that the memory maps in this section are for reference and are not intended to accurately illustrate the physical page length of each User Memory configuration. The physical page length is equal to the maximum number of bytes that can be written with a standard write command. The Write User Zone command will not write data across page boundaries; each physical page must be written with a separate command.

Figure C-1. AT88SC0104CRF Memory Map for 1 Kbit User Memory

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								

Figure C-2. AT88SC0204CRF Memory Map for 2 Kbit User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	64 bytes							
	-								
	$38								
User 1	$00								
	-	64 bytes							
	-								
	$38								
User 2	$00								
	-	64 bytes							
	-								
	$38								
User 3	$00								
	-	64 bytes							
	-								
	$38								

Figure C-3. AT88SC0404CRF Memory Map for 4 Kbit User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	128 bytes							
	-								
	$78								
User 1	$00								
	-	128 bytes							
	-								
	$78								
User 2	$00								
	-	128 bytes							
	-								
	$78								
User 3	$00								
	-	128 bytes							
	-								
	$78								

Figure C-4. AT88SC0808CRF Memory Map for 8 Kbit User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	128 bytes							
	-								
	$78								
User 1	$00								
	-	128 bytes							
	-								
	$78								
User 2	$00								
	-	128 bytes							
	-								
	$78								
User 3	$00								
	-	128 bytes							
	-								
	$78								
User 4	$00								
	-	128 bytes							
	-								
	$78								
User 5	$00								
	-	128 bytes							
	-								
	$78								
User 6	$00								
	-	128 bytes							
	-								
	$78								
User 7	$00								
	-	128 bytes							
	-								
	$78								

Figure C-5. AT88SC1616CRF Memory Map for 16 Kbit User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	128 bytes							
	$78								
User 1	$00								
	-	128 bytes							
	$78								
User 2	$00								
	-	128 bytes							
	$78								
User 3	$00								
	-	128 bytes							
	$78								
User 4	$00								
	-	128 bytes							
	$78								
User 5	$00								
	-	128 bytes							
	$78								
User 6	$00								
	-	128 bytes							
	$78								
User 7	$00								
	-	128 bytes							
	$78								
User 8	$00								
	-	128 bytes							
	$78								
User 9	$00								
	-	128 bytes							
	$78								
User 10	$00								
	-	128 bytes							
	$78								

Figure C-5. AT88SC1616CRF Memory Map for 16 Kbit User Memory (Continued)

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 11	$00								
	-	128 bytes							
	$78								
User 12	$00								
	-	128 bytes							
	$78								
User 13	$00								
	-	128 bytes							
	$78								
User 14	$00								
	-	128 bytes							
	$78								
User 15	$00								
	-	128 bytes							
	$78								

Figure C-6. AT88SC3216CRF Memory Map for 32 Kbit User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	256 bytes							
	$F8								
User 1	$00								
	-	256 bytes							
	$F8								
User 2	$00								
	-	256 bytes							
	$F8								
User 3	$00								
	-	256 bytes							
	$F8								
User 4	$00								
	-	256 bytes							
	$F8								
User 5	$00								
	-	256 bytes							
	$F8								
User 6	$00								
	-	256 bytes							
	$F8								
User 7	$00								
	-	256 bytes							
	$F8								
User 8	$00								
	-	256 bytes							
	$F8								
User 9	$00								
	-	256 bytes							
	$F8								
User 10	$00								
	-	256 bytes							
	$F8								

Figure C-6. AT88SC3216CRF Memory Map for 32 Kbit User Memory (Continued)

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 11	$00								
	-	256 bytes							
	$F8								
User 12	$00								
	-	256 bytes							
	$F8								
User 13	$00								
	-	256 bytes							
	$F8								
User 14	$00								
	-	256 bytes							
	$F8								
User 15	$00								
	-	256 bytes							
	$F8								

Figure C-7. AT88SC6416CRF Memory Map for 64 Kbit User Memory

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$000								
	-	512 bytes							
	$1F8								
User 1	$000								
	-	512 bytes							
	$1F8								
User 2	$000								
	-	512 bytes							
	$1F8								
User 3	$000								
	-	512 bytes							
	$1F8								
User 4	$000								
	-	512 bytes							
	$1F8								
User 5	$000								
	-	512 bytes							
	$1F8								
User 6	$000								
	-	512 bytes							
	$1F8								
User 7	$000								
	-	512 bytes							
	$1F8								
User 8	$000								
	-	512 bytes							
	$1F8								
User 9	$000								
	-	512 bytes							
	$1F8								
User 10	$000								
	-	512 bytes							
	$1F8								
User 11	$000								
	-	512 bytes							
	$1F8								

Figure C-7. AT88SC6416CRF Memory Map for 64 Kbit User Memory (Continued)

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 12	$000								
	-	512 bytes							
	$1F8								
User 13	$000								
	-	512 bytes							
	$1F8								
User 14	$000								
	-	512 bytes							
	$1F8								
User 15	$000								
	-	512 bytes							
	$1F8								

Annex D: Configuration Memory Maps

The Configuration Memory contains all of the system information used to configure the User Zones, plus 27 bytes of OTP memory that the customer can use to store data of any kind. The

data in the Configuration Memory is locked by programming fuses during the personalization process so that the PICC configuration cannot be changed by the end user.

Table D-1. CryptoRF Configuration Memory Characteristics

CryptoRF Part Number	Password Sets		Key Sets	OTP Memory	Transport Password	
		Set Number		Free for Customer Use	PW Index	Password
AT88SC0104CRF	4 Sets	0,1,2,7	4 Sets	27 Bytes	$07	$10 14 7C
AT88SC0204CRF	4 Sets	0,1,2,7	4 Sets	27 Bytes	$07	$20 C2 8B
AT88SC0404CRF	4 Sets	0,1,2,7	4 Sets	27 Bytes	$07	$30 1D D2
AT88SC0808CRF	8 Sets	0,1,2,3,4,5,6,7	4 Sets	27 Bytes	$07	$40 7F AB
AT88SC1616CRF	8 Sets	0,1,2,3,4,5,6,7	4 Sets	27 Bytes	$07	$50 44 72
AT88SC3216CRF	8 Sets	0,1,2,3,4,5,6,7	4 Sets	27 Bytes	$07	$60 78 AF
AT88SC6416CRF	8 Sets	0,1,2,3,4,5,6,7	4 Sets	27 Bytes	$07	$70 BA 2E

Access rights to the Configuration Memory are fixed in logic and are controlled by the security fuses. See Annex F for access control and fuse information. The Read System Zone and Write System Zone commands are used to access the Configuration Memory.

The contents of the Configuration Memory registers affect the functionality of CryptoRF and should be changed from their default configuration only after careful consideration. Incorrect or invalid settings can disable the device or prevent it from communicating with the PCD.

Configuration Memory registers marked as “Reserved” or RFU must not be changed and cannot be used for customer data. Only 27 bytes of OTP memory are available for general customer use, all other registers have assigned functionality. The 27 bytes of OTP memory available for customer use are described in Annex E: on page 69.

Figure D-1. Configuration Memory map for AT88SC0104CRF, AT88SC0204CRF, AT88SC0404CRF.

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	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	Reserved for Authentication and Encryption								Cryptography
$58									
$60									
$68									
$70									
$78									
$80									
$88									
$90	Reserved for Authentication and Encryption								Secret
$98									
$A0									
$A8									
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	Reserved								
$D0									
$D8									
$E0									
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

Figure D-2. Configuration Memory map for AT88SC0808CRF.

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	MTZ		Card Manufacturer Code				
$10	Lot History Code								Read Only
$18	DCR	Identification Number Nc							Access Control
$20	AR0	PR0	AR1	PR1	AR2	PR2	AR3	PR3	
$28	AR4	PR4	AR5	PR5	AR6	PR6	AR7	PR7	
$30	Reserved								
$38									
$40	Issuer Code								
$48									
$50	Reserved for Authentication and Encryption								Cryptography
$58									
$60									
$68									
$70									
$78									
$80									
$88									
$90	Reserved for Authentication and Encryption								Secret
$98									
$A0									
$A8									
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read3			
$D0	PAC	Write 4			PAC	Read 4			
$D8	PAC	Write 5			PAC	Read 5			
$E0	PAC	Write 6			PAC	Read 6			
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

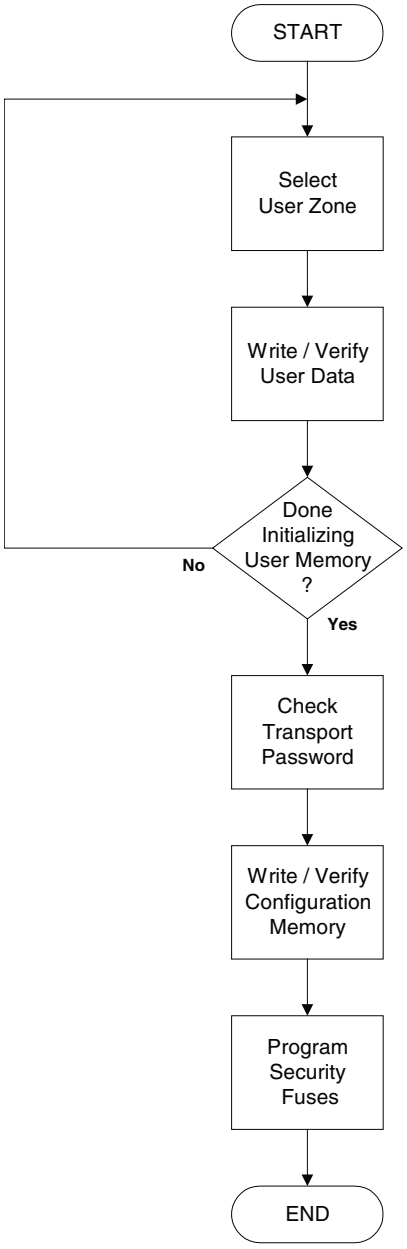
Figure D-3. Configuration Memory map for AT88SC1616CRF, AT88SC3216CRF, AT88SC6416CRF.

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	MTZ		Card Manufacturer Code				
$10	Lot History Code								Read Only
$18	DCR	Identification Number Nc							Access Control
$20	AR0	PR0	AR1	PR1	AR2	PR2	AR3	PR3	
$28	AR4	PR4	AR5	PR5	AR6	PR6	AR7	PR7	
$30	AR8	PR8	AR9	PR9	AR10	PR10	AR11	PR11	
$38	AR12	PR12	AR13	PR13	AR14	PR14	AR15	PR15	
$40	Issuer Code								
$48									
$50	Reserved for Authentication and Encryption								Cryptography
$58									
$60									
$68									
$70									
$78									
$80									
$88									
$90	Reserved for Authentication and Encryption								Secret
$98									
$A0									
$A8									
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read3			
$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									

Annex E: Device Personalization

CryptoRF is delivered with the user memory filled with $FF data and with all security features disabled. Before issuing a CryptoRF PICC to the end user, it is personalized with initial data and the security settings. The last step in the personalization process is to program the security fuses.

Figure E-1. Personalization Process Flowchart



E.1 User Memory Initialization

The user memory is initialized by using the Set User Zone command to select a User Zone, and writing the initial data with Write User Zone commands. The data is then verified with Read User Zone commands. Each User Zone is programmed in this manner.

E.2 Polling Response and OTP Memory Personalization

After initializing the user memory, the Configuration Memory is programmed with the polling response and OTP data. Figure E-2 shows the polling response registers in blue, OTP memory in green, and access control registers in gray. The Lot History Code register is factory programmed and cannot be changed.

There are 27 bytes of OTP memory available for customer use; these registers are shown in green in Figure E-2 and are described below. See Annex J for detailed information on configuration of the polling response registers. See Annex G for detailed information on configuration of the access control registers.

Figure E-2. System Zone Map showing the OTP and Polling Response Registers

<table>
<tr><th></th><th>$0</th><th>$1</th><th>$2</th><th>$3</th><th>$4</th><th>$5</th><th>$6</th><th>$7</th><th></th></tr>
<tr><td>$00</td><td colspan="4">PUPI</td><td colspan="4">APP</td><td rowspan="2">Anticollision</td></tr>
<tr><td>$08</td><td>RBmax</td><td>AFI</td><td colspan="2">MTZ</td><td colspan="4">Card Manufacturer Code</td></tr>
<tr><td>$10</td><td colspan="8">Lot History Code</td><td>Read Only</td></tr>
<tr><td>$18</td><td>DCR</td><td colspan="7">Identification Number Nc</td><td rowspan="6">Access Control</td></tr>
<tr><td>$20</td><td colspan="8" rowspan="4">Access Registers, Password Registers, and Reserved</td></tr>
<tr><td>$28</td></tr>
<tr><td>$30</td></tr>
<tr><td>$38</td></tr>
<tr><td>$40</td><td colspan="8" rowspan="2">Issuer Code</td></tr>
<tr><td>$48</td></tr>
</table>

Memory Test Zone (MTZ)

The MTZ is a 2 byte register with open read/write access for testing basic functionality of the PICC. Data written in the MTZ cannot be protected from being rewritten; this field should not be used for application data.

Card Manufacturer Code (CMC)

This 32-bit register, defined by the customer during personalization, is often used to store card manufacturer lot codes. This OTP register may contain any value; it is an information field that does not affect functionality.

Lot History Code

This 64-bit register is defined by Atmel. This code contains manufacturing traceability data and cannot be modified.

Identification Number Nc

This 56-bit register, defined by the customer during personalization, is often used to store card ID numbers. This OTP register may contain any value; it is an information field that does not affect functionality.

Issuer Code

The 128-bit Issuer Code register is defined by the customer during personalization. This OTP register may contain any value; it is an information field that does not affect functionality.

E.3 Transport Password Check

The Transport Password must be presented using the Check Password command prior to writing the Configuration Memory. The Transport Password for each CryptoRF device is shown in Table E-1. The Transport Password is the same for every device with the same base part number, it is never changed.

Table E-1. CryptoRF Transport Passwords

CryptoRF Part Number	Transport Password	
	PW Index	Password
AT88SC0104CRF	$07	$10 14 7C
AT88SC0204CRF	$07	$20 C2 8B
AT88SC0404CRF	$07	$30 1D D2
AT88SC0808CRF	$07	$40 7F AB
AT88SC1616CRF	$07	$50 44 72
AT88SC3216CRF	$07	$60 78 AF
AT88SC6416CRF	$07	$70 BA 2E

E.4 Security Fuse Programming

Three security fuses are programmed at the end of the personalization process to lock the PICC configuration. The Write Fuse Byte option of the Write System Zone command is used to program the fuses. A fourth fuse, SEC, is already programmed by Atmel before CryptoRF leaves the factory. The fuses can only be programmed in the specified order.

The security fuse programming sequence is as follows:

1. Send Write System Zone command with: PARAM = $01, ADDR = $06, L = $00, DATA = $00 to program the FAB fuse.
2. Send Write System Zone command with: PARAM = $01, ADDR = $04, L = $00, DATA = $00 to program the CMA fuse.
3. Send Write System Zone command with: PARAM = $01, ADDR = $00, L = $00, DATA = $00 to program the PER fuse.

The response to each Write System Zone command should be ACK, and the fuse byte contents will be returned in the STATUS byte. After all three fuses are programmed, the device configuration is locked and personalization is complete.

Annex F: Security Fuses

There are four fuses which control access to the Configuration Memory. One fuse (SEC) is programmed by Atmel before CryptoRF leaves the factory; the remaining three fuses are programmed during the personalization process. Once a fuse is programmed, it can never be changed.

These fuses do not control access to the user memory; user memory access rights are defined in the Access Registers. The security fuses are used to lock the state of the Access Registers, passwords, and other configuration data during the personalization process so that they cannot be changed after a card is issued.

F.1 Reading the Security Fuses

To read the fuses send the Read System Zone command with PARAM = $01, ADDR = $FF, L = $00. The CryptoRF response will contain one data byte, the fuse byte. A value of 0b indicates the fuse has been programmed. Bits 4 to 7 of this byte are not used as security fuses and are reserved by Atmel.

Figure F-1. Coding of the data byte received when reading the fuse byte.

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

F.2 Programming the Fuse Bits

Three security fuses are programmed at the end of the personalization process to lock the PICC configuration. The Write Fuse Byte option of the Write System Zone command is used to program the fuses. A fourth fuse, SEC, is already programmed by Atmel before CryptoRF leaves the factory. The fuses can only be programmed in the specified order.

The security fuse programming sequence is as follows:

4. Send Write System Zone command with: PARAM = $01, ADDR = $06, L = $00, DATA = $00 to program the FAB fuse.
5. Send Write System Zone command with: PARAM = $01, ADDR = $04, L = $00, DATA = $00 to program the CMA fuse.
6. Send Write System Zone command with: PARAM = $01, ADDR = $00, L = $00, DATA = $00 to program the PER fuse.

The response to each Write System Zone command should be ACK, and the fuse byte contents will be returned in the STATUS byte. After all three fuses are programmed, the device configuration is locked.

F.3 Configuration Memory Access Control

Table F-1 shows the Configuration Memory access conditions for each of the security fuse settings. The left column contains the name of the register area in the Configuration Memory map. The next column indicates if that row applies to Read System Zone commands or Write System Zone commands. The four columns to the right show the security fuse names.

The default state of the fuses when CryptoRF leaves the factory is SEC = 0b and the remaining three fuses set to 1b. The SEC fuse column in Table F-1 shows the access conditions for this fuse state. The FAB fuse column shows the access conditions for FAB = 0b. The CMA fuse col-

umn shows the access conditions for CMA = 0b. The PER fuse column shows the access conditions for PER = 0b.

Table F-1. Configuration Memory Access control by Security Fuse State.

Registers	Operation	Fuse			
		SEC = 0b	FAB = 0b	CMA = 0b	PER = 0b
Anticollision (Except MT2 and CMC)	*Read*	Open	Open	Open	Open
	Write	Transport PW	Forbidden	Forbidden	Forbidden
Memory Test Zone (MTZ)	*Read*	Open	Open	Open	Open
	Write				
Card Manufacturer Code (CMC)	*Read*	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Forbidden	Forbidden
Read Only (Lot History Code)	*Read*	Open	Open	Open	Open
	Write	Forbidden	Forbidden	Forbidden	Forbidden
Access Control	*Read*	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Transport PW	Forbidden
Cryptography (Except Encryption Key S)	*Read*	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Transport PW	Forbidden
Encryption Keys (S)	*Read*	Transport PW	Transport PW	Transport PW	Forbidden
	Write				
Secret	*Read*	Transport PW	Transport PW	Transport PW	Forbidden
	Write				
Passwords	*Read*	Transport PW	Transport PW	Transport PW	Write PW
	Write				
Password Attempts Counters (PAC)	*Read*	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Transport PW	Write PW
Forbidden	*Read*	Forbidden	Forbidden	Forbidden	Forbidden
	Write				

The register access conditions in Table F-1 are color coded. Open access is indicated by green. No access permitted is indicated by magenta. If access is restricted, then the field is yellow.

For registers with restricted access, the requirement to gain access is indicated by the text. The text “Transport PW” indicates that if the Transport Password is validated using the Check Password command, then access is granted. The text “Write PW” indicates that if the Write Password of a password set is validated using the Check Password command, then access is granted to the PAC registers and password registers for that password set only.

Annex G: Configuration of Password and Access Control Registers

There are two types of configuration registers in CryptoRF, User Zone access control registers, and device configuration registers. The User Zone access control registers set the access requirements for a single User Zone. The Device Configuration Register (DCR) selects optional behaviors for the PICC. Both types of registers are described in this annex.

G.1 User Zone Configuration Options

Access to each User Zone in the CryptoRF user memory is controlled by two registers in the Configuration Memory. The Access Register controls the access conditions for the User Zone. The Password Register controls the password set assigned to the User Zone. The default setting for these registers sets the security requirement to open access, no security features active, for all User Zones.

Each set of User Zone access control registers has a name matched to the User Zone name. For example, User Zone 1 is controlled by AR1 and PR1, User Zone 2 is controlled by AR2 and PR2. User Zone i is controlled by ARi and PRi.

G.1.1 Access Registers (AR)

There is one Access Register for each User Zone in the user memory. The default state of this register is $FF, which disables all of the optional security features.

Figure G-1. Bit definitions for the User Zone Access Registers.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
PM1	PM0	Reserved			WLM	MDF	PGO

The Access Register definition is shown in Figure G-1. Bits 3, 4, and 5 are reserved for control of the authentication and encryption modes and are not described in this document. The functionality of the remaining 5 bits is described below. Changes to the AR registers are effective immediately.

PM: Password Mode selection bits.

The PM0 and PM1 bits control the password requirements for the User Zone as shown in Table G-1 below. By default, no password is required for access to the User Zone. If PM = 10b, then write password verification is required for write access; read access does not require any password. If PM = 01b or 00b, then write password verification is required for read/write access and read password verification is required for read-only access. The password set assigned to the zone is specified in the Password Register.

Table G-1. Coding of the Password Mode bits of the Access Register.

PM1	PM0	Access
1	1	No Password Required
1	0	Write Password Required
0	1	Read and Write Passwords Required
0	0	

WLM: Write Lock Mode control.

By default the Write Lock Mode is disabled. If WLM = 0b then Write lock Mode is enabled and the user zone is effectively divided into 8 byte pages with the first byte of each page controlling write access to all 8 bytes. Figure G-2 shows an example of WLM on two contiguous pages.

Figure G-2. Example of byte level access control using the Write Lock Mode.

Page	$0	$1	$2	$3	$4	$5	$6	$7	< Address
$00	11011001 b	$xx	$xx	$xx	$xx	$xx	$xx	$xx	< Data
		locked	locked			locked			< Status

Page	$8	$9	$A	$B	$C	$D	$E	$F	< Address
$08	10101010 b	$xx	$xx	$xx	$xx	$xx	$xx	$xx	< Data
	locked		locked		locked		locked		< Status

The first byte of each virtual 8 byte page is called the Write Lock Byte. Each bit of the Write Lock Byte controls the locked status of one byte in the page. Write access is forbidden to a byte if its associated lock bit is set to 0b. Bit 7 controls byte 7, bit 6 controls byte 6, etc. Note that when WLM is enabled, Write User Zone commands are restricted to a length of one byte.

MDF: Modify Forbidden mode control.

By default the Modify Forbidden mode is disabled. If MDF = 0b then Modify Forbidden mode is enabled and no write access is allowed to the User Zone. The User Zone effectively becomes Read Only Memory (ROM).

PGO: Program Only mode control.

By default the Program Only mode is disabled. If PGO = 0b then data within the User Zone may be changed from 1b to 0b, but never from 0b to 1b. Note that when PGO is enabled, Write User Zone commands are restricted to a length of one byte.

G.1.2 Password/Key Registers (PR)

There is one Password/Key Register for each User Zone in the user memory. The default state of this register is $FF.

Figure G-3. Bit definitions for the User Zone Password/Key Registers.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Reserved					PW2	PW1	PW0

The Password/Key Register bit definitions are shown in Figure G-3. Bits 3 thru 7 are reserved for control of the authentication and encryption modes and are not described in this document. Changes to the PR registers are effective immediately.

PW: Password Set selection bits.

The Password Set selection bits control the password set assigned to a User Zone. Table G-2 and Table G-3 show the coding of these register bits. Any number of PR registers can point to the same password set, allowing multiple User Zones to use the same password set.

Table G-2. Coding of the Password Set select bits for 1K, 2K, and 4K bit CryptoRF devices.

PW2	PW1	PW0	Password Set
0	0	0	0
0	0	1	1
0	1	0	2
1	1	1	7
All Other Values Are Not Supported			

Table G-3. Coding of the Password Set select bits for 8K bit and larger CryptoRF devices.

PW2	PW1	PW0	Password Set
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

G.2 Device Configuration Options

There are a few configuration options which affect the overall behavior of the CryptoRF PICC. These options are contained in the Device Configuration Register (DCR).

G.2.1 Device Configuration Register (DCR)

There is one Device Configuration Register in each PICC. The default state of this register is $FF, which disables all of the optional features.

Figure G-4. Bit definitions for the Device Configuration Register

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
SME	Reserved		ETA	EGTL	*RFU*	*RFU*	*RFU*

The DCR register definition is shown in Figure G-4. Bits 5, and 6 are reserved for control of the authentication and encryption modes and are not described in this document. Bits 0, 1, and 2 are reserved for future use. Changes to the DCR are effective at the next POR or anticollision sequence.

SME: Supervisor Mode Enable control.

By default the Supervisor Mode is disabled. If SME = 0b then Supervisor Mode is enabled and Password Write 7 becomes the Supervisor Password. Successful verification of the Supervisor Password grants read and write access to all passwords and Password Attempt Counters (PACs), allowing the passwords to be changed and PACs to be reset.

ETA: Extended Trials Allowed control.

By default the Extended Trials Allowed option is disabled. If this option is enabled by setting ETA = 0b then the maximum number of password trials is increased to permit a maximum of eight password verification attempts before a password is locked. If ETA is disabled then only four password attempts are permitted.

EGTL: Extra Guard Time Length control.

By default the Extra Guard Time Length option is disabled, which maximizes RF communication speed. This option controls the Extra Guard Time (EGT) for all data transmitted by the PICC. The default setting of EGTL = 0b selects zero ETUs of EGT. Setting EGTL = 1b selects two ETUs of EGT for all transmissions. The EGTL option does not affect EGT requirements for data transmitted by the reader. See annex L for information about EGT.

Annex H: Using Password Security

CryptoRF contains security options that can be enabled by the customer at personalization. By default no security is enabled, allowing CryptoRF to operate as a simple RFID EEPROM memory. Enabling password security on a User Zone restricts access to the data to users with knowledge of the password.

H.1 Communication Security

Communication between the PICC and reader operates in three security modes. The Normal mode allows communication of all types of data in the clear. Authentication mode encrypts only passwords. Encryption mode encrypts both user data and passwords. The default communication mode is Normal mode.

Table H-1. CryptoRF Communication Security Options.

Communication Mode	User Data	System Data	Passwords
Normal	clear	clear	clear
Authentication	clear	clear	encrypted
Encryption	encrypted	clear	encrypted

As shown in Table H-1, passwords sent by the Host to CryptoRF in Normal communication mode are communicated in the clear, without being encrypted. In the Authentication or Encryption communication modes passwords are encrypted.

H.2 Transport Password

The Transport Password protects the Configuration Memory contents on all CryptoRF devices from accidental changes. All CryptoRF devices are shipped from Atmel with a Transport Password stored in password register Write 7. No changes to the Configuration Memory are permitted unless the Transport Password has been verified using the Check Password command.

Table H-2. CryptoRF Family Password Characteristics and Transport Passwords

CryptoRF Part Number	Password Sets		Transport Password	
		Set Number	PW Index	Password
AT88SC0104CRF	4 Sets	0,1,2,7	$07	$10 14 7C
AT88SC0204CRF	4 Sets	0,1,2,7	$07	$20 C2 8B
AT88SC0404CRF	4 Sets	0,1,2,7	$07	$30 1D D2
AT88SC0808CRF	8 Sets	0,1,2,3,4,5,6,7	$07	$40 7F AB
AT88SC1616CRF	8 Sets	0,1,2,3,4,5,6,7	$07	$50 44 72
AT88SC3216CRF	8 Sets	0,1,2,3,4,5,6,7	$07	$60 78 AF
AT88SC6416CRF	8 Sets	0,1,2,3,4,5,6,7	$07	$70 BA 2E

H.3 The Password and PAC Registers

Each password set, along with it's associated Password Attempt Counters is stored in an 8 byte segment in the Password section of the Configuration Memory. Figure H-1 illustrates password set "z" in the Configuration Memory map. The Write Password and Write Password PAC are stored in the lower four bytes, while the Read Password and Read Password PAC are stored in the upper four bytes.

Figure H-1. Password Set Register Format

	$0	$1	$2	$3	$4	$5	$6	$7
Addr	PAC	PW Write z			PAC	PW Read z		

PAC	PW1	PW2	PW3	PAC	PW1	PW2	PWS

Each password register contains the three byte password that is compared with the three byte password that is sent for verification with the Check Password command. The storage locations of the three password bytes is illustrated in the bottom half of Figure H-1.

Table H-3. Password Attempt Counter Coding for the Default Configuration

PAC Register	Description
$FF	No Failed Attempts
$EE	1 Failed Attempt
$CC	2 Failed Attempts
$88	3 Failed Attempts
$00	4 Failed Attempts (LOCK)
All Other Values Are Not Supported	

Table H-4. Password Attempt Counter Coding for the Extended Trials Allowed Configuration

PAC Register	Description
$FF	No Failed Attempts
$FE	1 Failed Attempt
$FC	2 Failed Attempts
$F8	3 Failed Attempts
$F0	4 Failed Attempts
$E0	5 Failed Attempts
$C0	6 Failed Attempts
$80	7 Failed Attempts
$00	8 Failed Attempts (LOCK)
All Other Values Are Not Supported	

The Password Attempt Counters contain a value which indicates how many unsuccessful password verification attempts have been made using the Password Index of the corresponding password. Table H-3 and Table H-4 show coding of the PAC register. DCR register bit ETA selects the number of password attempt that are permitted; the default configuration allows four attempts, ETA = 0b allows eight attempts. If the PAC reaches the maximum count, then the corresponding password is locked and all subsequent Check Password commands will fail.

H.4 Password Security Options

Password security for a User Zone is enabled by programming the Access Register for the zone. A Password Set is assigned to the User Zone by programming the Password/Key Register for the zone. Configuration of the registers is described in annex G.

Table H-5. Coding of the Password Mode bits of the Access Register.

PM1	PM0	Access
1	1	No Password Required
1	0	Write Password Required
0	1	Read and Write Passwords Required
0	0	

Table H-5 shows the available password security options. The default setting of PM=00b disables password security. The remaining two options enable password security for either writes only, or for both reads and writes.

If PM = 10b, then the Write Password is required to be verified before a Write User Zone command will be accepted. Data reads are not restricted in this configuration.

If read and write password security is enabled by setting PM = 01b or PM = 00b, then verification of the Read Password allows access to data with the Read User Zone command; however no write access is permitted. Verification of the Write Password allows access to the data with either Read User Zone or Write User Zone commands.

H.5 Password Verification

A password is sent for verification using the Check Password command as shown in figure H-2. The Password Index identifies the Password Register that the password will be compared against. If the passwords match, then the PICC will latch the verification status as PASS along with the Password Index in an internal register, write the PAC to $FF, and return an ACK in the response.

The internal password security status register maintains it's contents until the PICC is reset or some other event causes them to be changed. For example, sending another Check Password command will update these registers to reflect the success or failure of the new password verification event. Note that only one password is active at any time, and only the status of the most recent password verification event is stored in the PICC.

If multiple User Zones are assigned the same Password Set, then a single Check Password command will provide access to all of these User Zones. Note that it does not matter if the Set User Zone command is sent before or after a Check Password command. The currently selected User Zone is stored in a register that is independent of the password security status register.

Figure H-2. Check Password Command and Response

	Reader	PICC
Command >	CID | $C Password Index PW 1 PW 2 PW 3 CRC1 CRC2	
Echo Command >		CID | $C ACK/NACK STATUS CRC1 CRC2

If a Check Password command fails, then the PICC returns a NACK and a non-zero Status byte in the response. This Status byte reports the reason for failure of the operation. See the Check Password command section of this specification for a description of the Status codes.

Table H-6. Check Password Command ACK/NACK Coding.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Response Decode
0	0	0	0	0	0	0	0	ACK
0	0	0	0	0	0	0	1	NACK, See STATUS byte for cause
Password Attempts Counter				0	0	0	1	NACK, Check Password Attempt Failure

A Check Password response NACK can be coded two different ways, depending on the reason for failure. If failure of the Check Password command results in the Password Attempt Counter being incremented, then the NACK byte will contain an embedded code indicating the number of failed attempts. This special NACK will contain one of the following values: $11, $21, $31, $41, $51, $61, $71, $81. The upper nibble of the NACK byte is the number of failed attempts (1 to 8 failures), while the lower nibble is the NACK code $1.

H.6 Changing Passwords

To change a password after the personalization procedure is complete and the card configuration has been locked by programming the security fuses, it is necessary to successfully verify the Write Password of a password set using the Check Password command. The Read Password and Write Password registers and PACs can then be written using a Write System Zone command, and verified using the Read System Zone command.

If the PAC for the Write Password has reached the attempt count limit, then the Write Password will be locked and it is not possible to change the passwords or PACs in this set. However if the optional Supervisor Mode has been enabled, then the Supervisor Password can be used to enable write access to the passwords unless the Supervisor Password is also locked.

H.7 Supervisor Password

Supervisor Mode is an optional feature that can be enabled by programming SME = 0b in the DCR register. In Supervisor Mode a Supervisor Password is enabled that grants read and write access to all of the password sets and PACs. Password Write 7 is the Supervisor Password if SME = 0b.

If the Supervisor Password is successfully verified, then it is possible to write any of the passwords and PACs. This allows passwords to be easily changed in the field, and for PACs to be reset to $FF (no unsuccessful attempts) by writing the registers using the Write System Zone command.

When a PICC is configured with SME = 0b, it is recommended that Password Set 7 be reserved for the Supervisor Password. User Zones using password security should be configured to use other password sets. If a PICC is configured in this manner, then it is unlikely that the PAC for Password Write 7 will accidentally become locked (due to too many unsuccessful attempts). If the PAC for Password Write 7 is locked, then all subsequent attempts to verify the Supervisor Password will fail.

Supervisor Mode changes the Configuration Memory access requirements for the Password section of the memory only. Enabling Supervisor Mode does not change the access requirements for any other configuration registers.

Annex I: Understanding Anti-Tearing

Anti-tearing is an optional feature that protects a write operation from being corrupted due to PICC power loss during the write operation. This feature can be enabled as needed by the PCD during a transaction, it is not controlled by a configuration register.

I.1 Tearing Explained

A tearing attack on a Smartcard transaction involves quickly removing a card from the reader before a transaction has been completed. The object of a tearing attack is to remove the card from the reader after the Host application has granted access to a product, but before the cost of the product has been deducted from the value stored on the card.

Both contact and contactless Smartcard transactions may be attacked in this manner. A tearing attack often results in corruption of a portion of the data stored in the Smartcard.

Tearing attacks can be prevented from succeeding by careful application software development; if access to a product is not granted until after a Smartcard value debit has occurred, then the attacker cannot achieve his objective. However data corruption can occur if any Smartcard transaction is interrupted due to power loss.

I.2 CryptoRF Anti-Tearing

CryptoRF is designed with an anti-tearing feature that prevents data corruption in the event a memory write operation is interrupted. Activating the anti-tearing feature impacts both the transaction time and the memory write endurance of the PICC, so if should be activated only for critical data write operations.

Figure I-1 illustrates how a CryptoRF PICC performs an anti-tearing write. A CryptoRF anti-tearing write is a four step process. The data is written to a buffer EEPROM memory before being written to the final EEPROM memory location. The EEPROM Anti-Tearing Flag indicates if an anti-tearing write is in progress, or is completed.

The Anti-Tearing Flag is checked each time the PICC is powered up. If the flag indicates a write was in progress, then the anti-tearing write will be completed before the PICC is allowed to accept any commands.

The memory address and data are written to a buffer EEPROM in step 1, followed by writing the Anti-Tearing Flag in Step 2. In step 3 the data in the buffer EEPROM is written to the address sent with the write command (the final EEPROM memory location). The Anti-Tearing flag is cleared in step 4, and the ACK response is returned to the PCD.

If power is interrupted before step 2 is completed, then the write operation fails; the EEPROM contents are unchanged, and the Anti-Tearing Flag is not set to indicate an anti-tearing write is in progress. If power is interrupted after step 2 is complete, then the Anti-Tearing flag is set; when the PICC is next powered up, the anti-tearing write will be completed as part of the POR process. If power is interrupted during step 3 or 4, the Anti-Tearing Flag will be set and the write will be completed on the next POR.

Figure I-1. CryptoRF Anti-Tearing Write Process

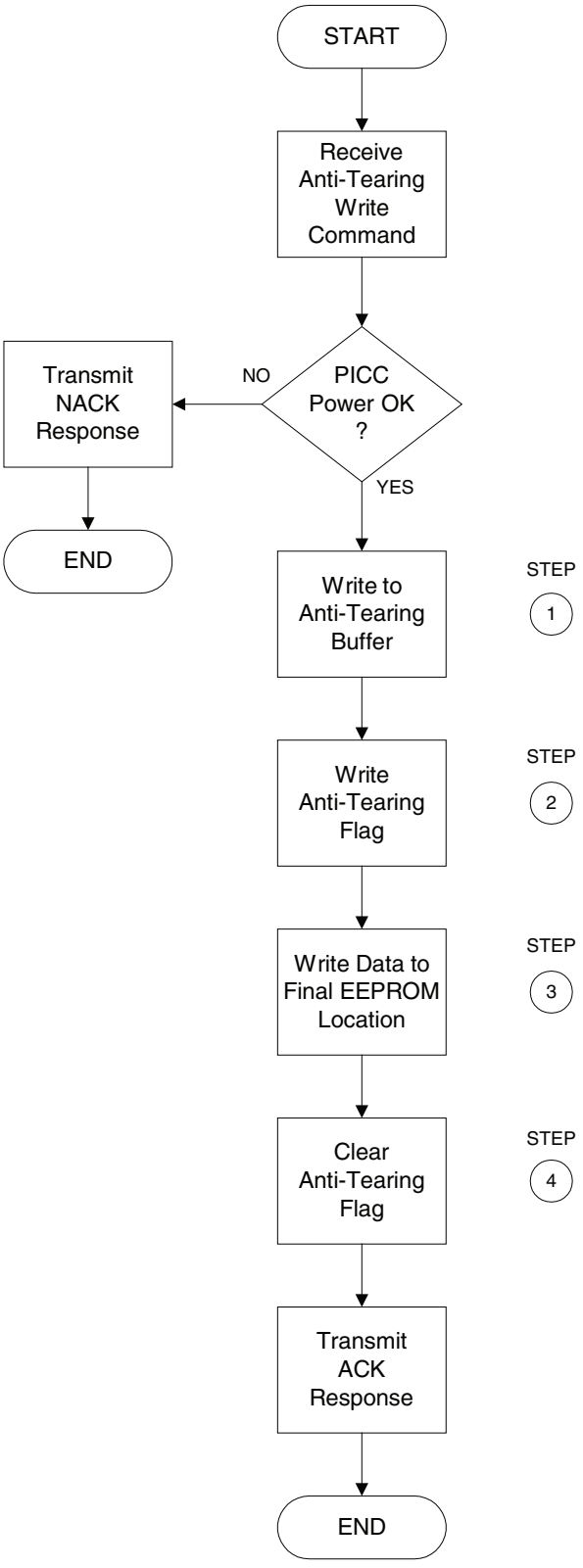


Table I-1 shows the consequences of a tearing attack occurring at each step during an anti-tearing write. The EEPROM contents at the address being written will either remain unchanged, or will be written with the new data. The EEPROM is not corrupted by power interruption during an anti-tearing write operation.

Table I-1. Consequences of a Tearing Event during an Anti-Tearing Write

Step	Description	Result if Power is Interrupted Mid-Step
1	Write Buffer Memory	Original EEPROM Contents are Unchanged
2	Write Anti-Tearing Flag	Original EEPROM Contents are Unchanged
3	Write Final Memory	Anti-Tearing Write Completes on POR
4	Clear Anti-Tearing Flag	Anti-Tearing Write Completes on POR

I.3 Performance Impact of Anti-Tearing

Anti-tearing impacts the CryptoRF write transaction time in two ways. First, the maximum length of a write command is limited to 8 bytes when anti-tearing is active. Second, the response time of a write command is increased by approximately four times due to additional EEPROM memory writes which occur when anti-tearing is active.

If anti-tearing is used to write 8 bytes of data, the net result is an increase in the transaction time of only 5 milliseconds. When large amounts of data are written, the increase in transaction time is significant. Writing the entire 128 byte User Zone on AT88SC0404CRF takes 147 milliseconds with anti-tearing, but only 41 milliseconds without anti-tearing. Writing the entire 256 byte User Zone on AT88SC3216CRF takes 292 milliseconds with anti-tearing, but only 54 milliseconds without anti-tearing.

Table I-2. CryptoRF Family Write Characteristics with Anti-Tearing

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88SC0104CRF	1 to 16 bytes	1 to 8 bytes
AT88SC0204CRF	1 to 16 bytes	1 to 8 bytes
AT88SC0404CRF	1 to 16 bytes	1 to 8 bytes
AT88SC0808CRF	1 to 16 bytes	1 to 8 bytes
AT88SC1616CRF	1 to 16 bytes	1 to 8 bytes
AT88SC3216CRF	1 to 32 bytes	1 to 8 bytes
AT88SC6416CRF	1 to 32 bytes	1 to 8 bytes

I.4 Reliability Impact of Anti-Tearing

Each byte of the CryptoRF EEPROM user memory and configuration memory is rated for 100k write cycles minimum. The entire memory can be written at least 100,000 times without wearing out any of the EEPROM memory bits.

Table I-3. CryptoRF Family Write Endurance with Anti-Tearing

Parameter	Min	Typ	Max	Units
Write Endurance (each Byte)	100,000			Write Cycles
Anti-Tearing Write Endurance	50,000			Writes

All anti-tearing write commands sent to a PICC are processed in a single buffer EEPROM memory before being written to the final EEPROM memory location. As a result, the write endurance for anti-tearing writes is a per-unit specification, not a per-byte specification. A minimum of 50,000 anti-tearing write commands can be processed without wearing out any of the buffer EEPROM bits, or the EEPROM Anti-Tearing Flag bits.

I.5 Activating Anti-Tearing

Anti-Tearing can be used for either User Zone or Configuration Memory writes. Activation of this optional feature is described in this section.

The Set User Zone command is used to activate the anti-tearing feature when writing the user memory. To turn anti-tearing on, send a Set User Zone command with bit 7 in the PARAM byte set to 1b. Any Write User Zone command that is received following anti-tearing activation will automatically use the anti-tearing write process. To turn anti-tearing off, send a Set User Zone command with bit 7 in the PARAM byte set to 0b. All subsequent Write User Zone commands will automatically use the normal write process.

Figure I-2. Coding of the PARAM byte of the Set User Zone command.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
AT	0	0	0	User Zone			

When writing the Configuration Memory the anti-tearing function is controlled by the PARAM byte of the Write System Zone command. Table I-3 shows the PARAM byte options. If the PARAM byte of the Write System Zone command is $80, then the anti-tearing write process is used. If the PARAM byte of the Write System Zone command is $00, then the normal write process is used.

Table I-4. PARAM byte options for the Write System Zone command.

Command	PARAM	ADDR	"L"	DATA
Write System Zone	$00	address	# of bytes - 1	"L + 1" bytes
Write System Zone w A/T	$80	address	# of bytes - 1	"L + 1" bytes
Write Fuse Byte	$01	fuse addr	$00	1 byte
All Other Values Are Not Supported				

Annex J: Personalization of the Anticollision Registers

There are several registers that define the polling response of CryptoRF, which are written during the personalization process. The ISO/IEC 14443 Part 3 requirements must be considered when programming these registers. Incorrect personalization of these registers may cause readers to reject cards or to become confused and unable to complete the transaction. This annex describes the requirements for programming the polling registers for operation with ISO/IEC 14443 compliant readers and systems.

J.1 Anticollision Procedure

The RF reader (PCD) searches for Type B cards by issuing REQB or WUPB polling commands. These commands contain an AFI (Application Family Identifier) code to poll for only cards with a matching AFI code. Applications supporting multiple cards may also poll using the Slot MARKER command. See Annex K for a detailed description of the anticollision procedures.

The answer to any of these polling commands is called the ATQB response. This response contains a card serial number (PUPI), which is used to select a specific card during the anticollision process, along with three protocol bytes. The protocol bytes tell the PCD what communication capabilities and options the card supports, and are used by the reader to configure itself for optimum communications with the card.

J.2 Anticollision Registers

The ATQB response of CryptoRF contains several values that are located in registers in the anticollision section of the System Zone (see Figure J-1). The values stored in the following registers are used during anticollision: PUPI, APP, RBmax, AFI.

Figure J-1. Memory Map of Anticollision Registers in the System Zone

<table>
<tr><th></th><th>$0</th><th>$1</th><th>$2</th><th>$3</th><th>$4</th><th>$5</th><th>$6</th><th>$7</th><th></th></tr>
<tr><td>$00</td><td colspan="4">PUPI</td><td colspan="4">APP</td><td rowspan="2">Anticollision</td></tr>
<tr><td>$08</td><td>RBmax</td><td>AFI</td><td colspan="2">MTZ</td><td colspan="4">Card Manufacturer Code</td></tr>
</table>

The REQB/WUPB polling command and response are shown in Figure J-2 with color-coding which matches Figure J-1. Nine bytes of the ATQB response are customer programmable on CryptoRF. In addition, the AFI code used for selection of cards for a particular application during anticollision is also customer configured.

Figure J-2. CryptoRF Response to an REQB or WUPB polling command.

	Reader	PICC
Command >	$05 AFI PARAM CRC1 CRC2	
ATQB Response >	$50	SUCCESS RESPONSE
	PUPI 0	System Zone Byte $00
	PUPI 1	System Zone Byte $01
	PUPI 2	System Zone Byte $02
	PUPI 3	System Zone Byte $03
	APP 0	System Zone Byte $04
	APP 1	System Zone Byte $05
	APP 2	System Zone Byte $06
	APP 3	System Zone Byte $07
	Protocol 1	$00
	Protocol 2	System Zone Byte $08
	Protocol 3	$51
	CRC1	
	CRC2	

The definitions of the polling configuration registers in the System Zone are listed below along with any restrictions which ISO/IEC 14443 Part 3 places on the register values.

Pseudo Unique PICC Identifier (PUPI)

PUPI is a 32 bit serial number defined by the customer during personalization; the PUPI is usually unique. This code is transmitted as part of the ATQB response during anticollision. PUPI may be set to any value.

Application Data (APP)

APP is an additional 32 bits of information transmitted as part of the ATQB response. This field is defined by the customer during personalization. The fourth byte is programmed by Atmel at the factory with a memory density code (see Figure J-1); this byte can be redefined by the card manufacturer if desired. APP may be set to any value.

Table J-1. Default Value of APP 3 Byte. This Register can be Changed.

Device Number	Density Code
AT88SC0104CRF	$02
AT88SC0204CRF	$12
AT88SC0404CRF	$22
AT88SC0808CRF	$33
AT88SC1616CRF	$44
AT88SC3216CRF	$54
AT88SC6416CRF	$64

Receive Buffer Max Code (RBmax)

This 8-bit register is transmitted as Protocol 2 byte of the ATQB response. This register is programmed by Atmel with the receive buffer maximum frame size code. This field can be reprogrammed by the customer during personalization if desired. The value of this protocol byte is restricted by ISO/IEC 14443 Part 3 to the values $00, $10, $20, $30, $40, $50, $60, $70, or $80 only. Use of an unapproved value in this register is likely to cause PCDs to malfunction.

The Protocol 2 byte of the ATQB response is defined in ISO/IEC 14443 Part 3, section 7.9 . This byte contains the Part 4 compliance code in the lower 4 bits and the code for the maximum frame size supported by the card in the upper 4 bits. CryptoRF must return a value of $0 in the Part 4 compliance bits to indicate the PICC does not support the optional ISO/IEC 14443 Part 4 Active State protocol. The coding of the card maximum frame size bits is shown in Figure J-2.

Table J-2. PICC Maximum Frame Size Codes defined in ISO/IEC 14443 Part 3.

Bit 7	Bit 6	Bit 5	Bit 4	Max Frame
0	0	0	0	16 Bytes
0	0	0	1	24 Bytes
0	0	1	0	32 Bytes
0	0	1	1	40 Bytes
0	1	0	0	48 Bytes
0	1	0	1	64 Bytes
0	1	1	0	96 Bytes
0	1	1	1	128 Bytes
1	0	0	0	256 Bytes

The PCD will store the lower 4 bits of ATQB protocol byte 2 in a register and echo it back to a selected PICC in the lower 4 bits of ATTRIB parameter byte 3. CryptoRF will not accept an ATTRIB command with a non-zero value in parameter byte 3. Note that intelligent PCDs will reject invalid ATQB responses and will not send invalid ATTRIB commands.

Table J-3. Default Value of RBmax. This Register should not be Changed.

Device Number	RBmax Code
AT88SC0104CRF	$10
AT88SC0204CRF	$10
AT88SC0404CRF	$10
AT88SC0808CRF	$10
AT88SC1616CRF	$10
AT88SC3216CRF	$30
AT88SC6416CRF	$30

Application Family Identifier (AFI)

This 8 bit register identifies the application family and subfamily. This field is defined by the card manufacturer and is used during the anticollision process to determine which cards will respond to an REQB or WUPB polling command. This value is expected to be a single fixed value for all cards used in a particular system.

The upper 4 bits are the application family and the lower 4 bits are the sub-family. The ISO/IEC 14443 Part 3 Type B application family definitions are shown in Figure J-6. The AFI register will accept any code, however only family codes of $0 to $F and subfamily codes of $1 to $F should be used. AFI Register values of $00, $10, $20, $30, $40, $50, $60, $70, $80, $90, $A0, $B0, $C0, $D0, $E0, and $F0 are prohibited and may cause PCDs to malfunction. Values defined as RFU are reserved for future definition by ISO and may not be supported by all readers. A card using an RFU value for the AFI is not compliant with ISO/IEC 14443 Part 3.

Table J-4. Application Family Codes as defined in ISO/IEC 14443 Part 3.

AFI High Bits	AFI Low Bits	Application Family	Examples
$0	“Y”	Proprietary	
$1	“Y”	Transport	Mass Transit, Bus, Airline...
$2	“Y”	Financial	Banking, Retail, Elec. Purse...
$3	“Y”	Identification	Access Control...
$4	“Y”	Telecomm	Telephony, GSM...
$5	“Y”	Medical	
$6	“Y”	Multimedia	Internet Services...
$7	“Y”	Gaming	
$8	“Y”	Data Storage	Portable Files...
$9 - $F	“Y”	RFU	not currently defined by 14443-3

Note: “Y” = $1 to $F

J.3 Summary

The CryptoRF anticollision registers provide customers with the capability to customize the response of a CryptoRF PICC to the polling commands. This polling response is used by the PCD to perform anticollision and to determine the communication capabilities of the PICC. Intelligent RF readers will reconfigure themselves based on the contents of the protocol bytes in ATQB and may malfunction if invalid values are returned by the card. For this reason, the values of the CryptoRF anticollision registers must be carefully selected using the guidelines in this annex.

Annex K: Understanding Anticollision

This section of the specification and the flow chart in Figure K-1 describe the Anticollision procedure for the CryptoRF family. The command and response definitions are detailed in the "Anticollision Command Definitions" section of this specification. For additional information on the anticollision command coding see section 7 of ISO/IEC 14443 Part 3 or Atmel Application note *Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards*.

When the PICC enters the 13.56 Mhz RF field of the host reader (PCD) it performs a power on reset (POR) function and waits silently for a valid Type B polling command. The CryptoRF PICC processes the anti-tearing registers as part of the POR process.

The PCD initiates the anticollision process by issuing an REQB or WUPB command. The WUPB command activates any card (PICC) in the field with a matching AFI code. The REQB command performs the same function, but does not affect a PICC in the Halt State. The REQB and WUPB commands contain an integer "N" indicating the number of Slots assigned to the anticollision process.

If "N" = 1 then all PICCs (with a matching AFI) respond with the ATQB response. If "N" is greater than one, then the PICC selects a random number "R" in the range of 1 to "N" ; if "R" = 1 then the PICC responds with ATQB. If "R" is greater than 1, then the PICC waits for a Slot MARKER command where the slot number "S" is equal to "R", then it responds with ATQB. The PCD polls all of the slots to determine if any PICC is present in the field.

The ATQB response contains a PUPI card serial number which is used to direct commands to a specific PICC during the anticollision process. When the PCD receives an ATQB response, it can respond with a matching HLTB command to Halt the PICC, or it can respond with a matching ATTRIB command to assign a Card ID Number (CID) and place the PICC in the Active State.

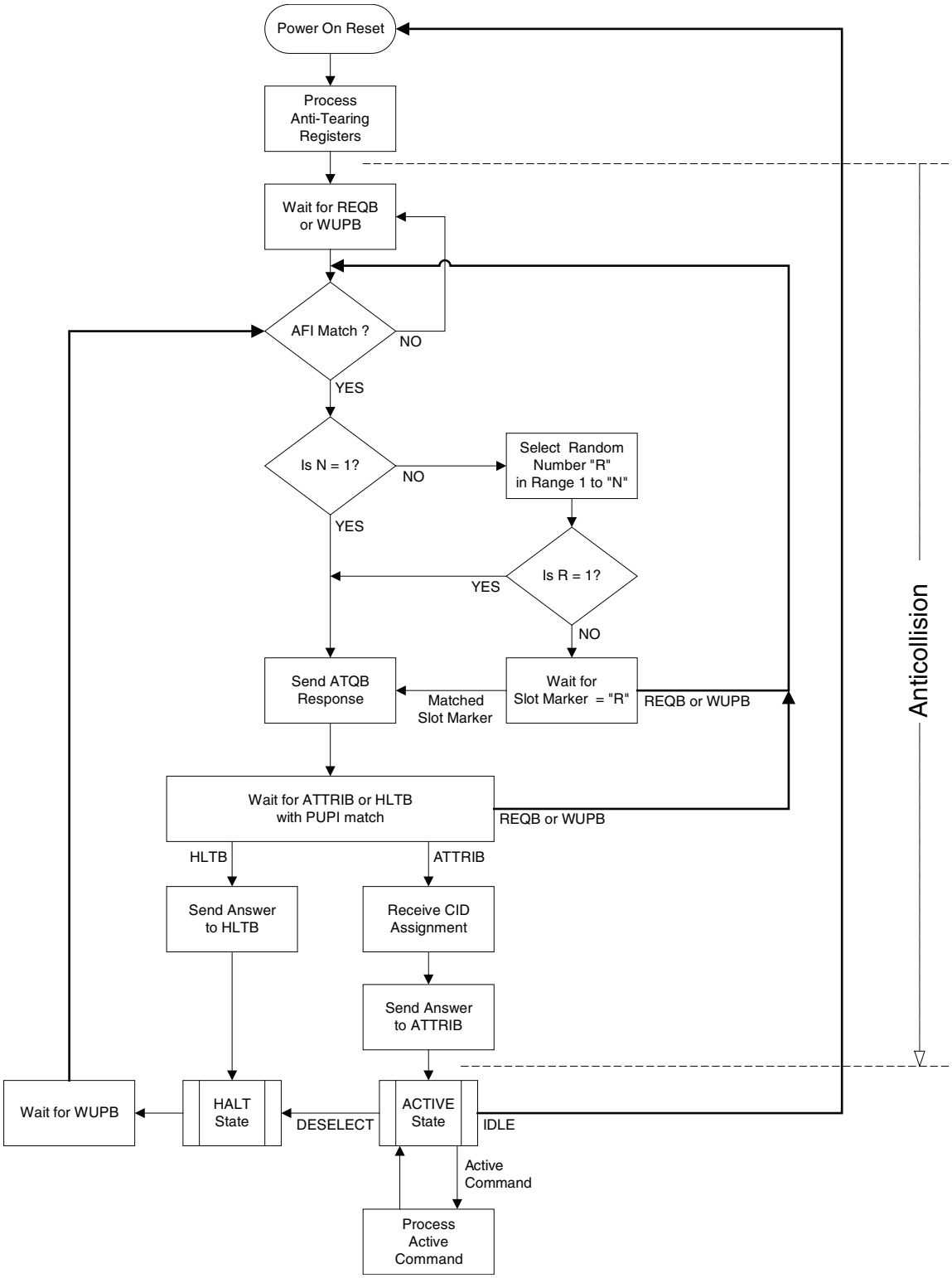
Once placed in the Active State the PICC is ready for transactions using the CryptoRF Active State commands. A PICC in the Active State ignores all commands that do not contain a CID number which matches the CID assigned by the ATTRIB command. A PICC in the Active State ignores all REQB, WUPB, Slot MARKER, ATTRIB, and HLTB commands.

When the PCD receives an ATQB response with a CRC error, then a collision is assumed to have occurred. Typically the PCD will complete transactions with any other PICCs in the field, and then place them in the Halt State using a DESELECT command. The PCD will then issue a new REQB command, causing each PICC in the field (with a matching AFI) that has not been Halted to select a new random number "R". This procedure resolves the conflict between the previously colliding PICCs, allowing the PCD to communicate with them.

The anticollision process continues in this manner until all PICCs in the field have completed their transactions. Any command received by the PICC with a CRC error is ignored.

Note that ISO/IEC 14443 Part 3 describes two anticollision options for Type B PICCs; the Timeslot option has been implemented in the CryptoRF family.

Figure K-1. Anticollision and State Transition Flow Chart



Annex L: The ISO/IEC 14443 Type B RF Signal Interface

L.1 RF Signal Interface

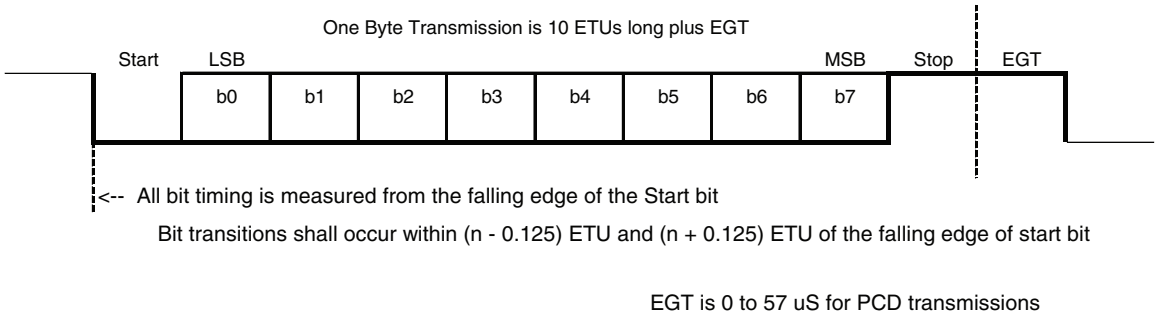
The CryptoRF communications interface is compliant with the ISO/IEC 14443 part 2 and part 3 requirements for Type B. Type B signaling utilizes 10 % amplitude modulation of the RF field for communication from the reader to the card with NRZ encoded data. Communication from card to reader utilizes BPSK load modulation of an 847.5 khz subcarrier with NRZ-L encoded data. The RF field is continuously on for Type B communications.

L.2 Data Format

Data communication between the card and reader is performed using an LSB first data format. Each byte of data is transmitted with a 0b start bit and a 1b stop bit as shown in Figure L-1. The stop bit, start bit, and each data bit are each one elementary time unit (ETU) in length (9.4395 microseconds).

Each byte transmission consists of a start bit, 8 data bits (LSB first), and a stop bit. Each byte may be separated from the next byte by extra guard time (EGT). The EGT may be zero or a fraction of an ETU. EGT cannot exceed 57 microseconds for data transmitted by the PCD. EGT for data transmitted by the CryptoRF PICC is programmed to either zero or 2 ETUs using the EGTL bit of the Device Configuration Register (DCR). The position of each bit is measured relative to the falling edge of the start bit.

Figure L-1. Byte transmission format requirements for type B communications.

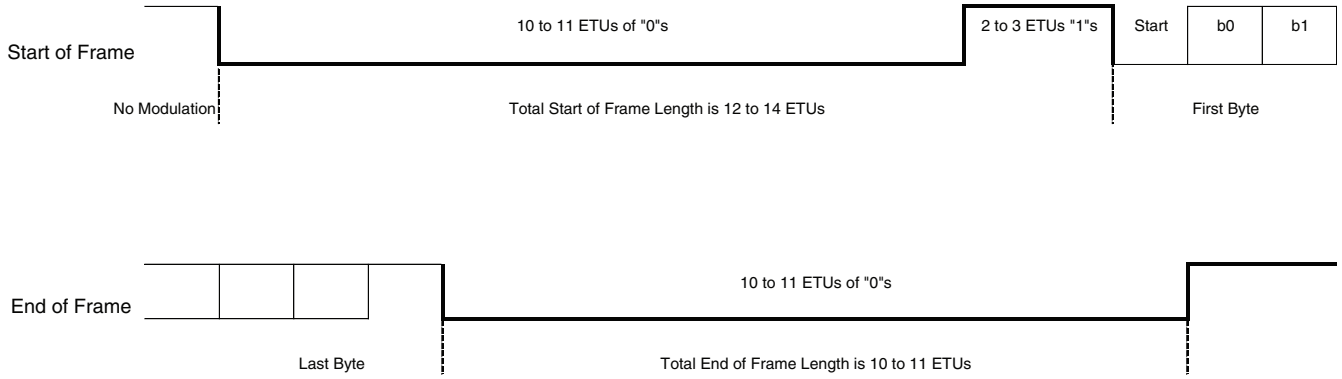


Despite the fact that data transmissions occur LSB first, all of the commands, data, and CRC bytes in ISO/IEC 14443 and in this specification are listed in the conventional manner, with MSB on the left and LSB on the right.

L.3 Frame Format

Data transmitted by the PCD or PICC is sent as frames. The frame consists of the start of frame (SOF), several bytes of information, and the end of frame (EOF). The SOF and EOF requirements are shown in Figure L-2.

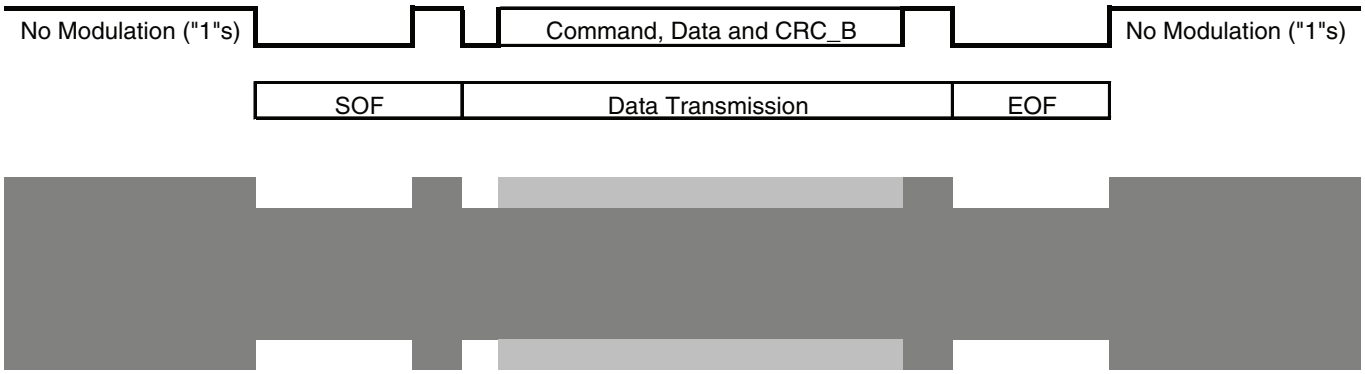
Figure L-2. Start of Frame (SOF) and End of Frame (EOF) format requirements.



L.4 Reader Data Transmission

The unmodulated 13.56 Mhz carrier signal amplitude which is transmitted when the reader is idle is defined as logical “1”, while the modulated signal level is defined as logical “0”. A frame transmitted by the reader consists of SOF, several bytes of data, a 2 byte CRC_B, and the EOF.

Figure L-3. Format of a frame transmitted by the reader to the card.

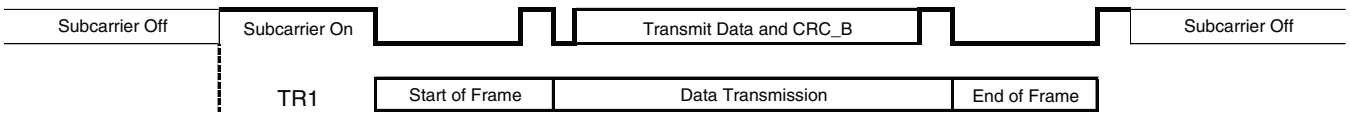


L.5 Card Data Transmission

The CryptoRF PICC waits silently for a command from the PCD after being activated by the RF field. After receiving a valid command from the PCD, the PICC is allowed to turn on the subcarrier only if it intends to transmit a complete response frame. The PICC response consists of TR1, SOF, several bytes of data followed by a 2 byte CRC_B, and the EOF. The subcarrier is turned off no later than 2 ETUs after the EOF. Figure L-4 shows the PICC frame format

When the subcarrier is turned on it remains unmodulated for a time period known as the synchronization time (TR1). The phase of the subcarrier during TR1 defines a logical one and permits the reader demodulator to lock on to the subcarrier signal. The subcarrier remains on until after the EOF transmission is complete. The TR1 transmitted by CryptoRF is 10 to 11 ETUs in duration for all responses.

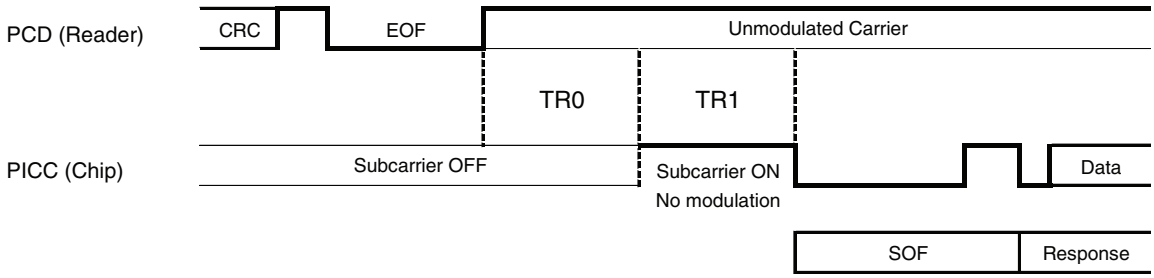
Figure L-4. Format of a frame transmitted by the PICC to the reader.



L.6 Response Timing

After the PICC receives a command from the PCD, it is not permitted to transmit a subcarrier during the guard time (TR0). The minimum guard time is 8 ETUs for all command responses. The maximum guard time is defined by the frame waiting time (FWT), except for the ATQB response (response to REQB or Slot MARKER polling commands) which has a maximum TR0 of 32 ETUs.

Figure L-5. ISO/IEC 14443 Response timing requirements for the card.



The FWT is the maximum time that a PICC requires to begin a response. The PICC transmits a parameter in the ATQB response to the polling command that tells the reader the worst case FWT. Typical response times for the CryptoRF are listed in Annex N of this specification. See Annex M for signal timing specifications.

The PCD is not permitted to modulate the RF field while waiting for a PICC to respond to a command. Modulation of the RF field during a memory read or write operation may corrupt the operation or cause reset of the PICC.

L.7 CRC Error Detection

A 2 byte CRC_B is required in each frame transmitted by the PICC or PCD to permit transmission error detection. The CRC_B is calculated on all of the command and data bytes in the frame. For encrypted data the encryption is performed prior to CRC_B calculation. The SOF, EOF, start bits, stop bits, and EGT are not included in the CRC_B calculation. The two byte CRC_B follows the data bytes in the frame.

Figure L-6. Location of the two CRC_B bytes within a frame.

SOF	K data bytes	CRC1	CRC2	EOF

The CRC_B polynomial is defined in ISO/IEC 14443 and ISO/IEC 13239 as $x^{16} + x^{12} + x^5 + x^0$. This is a hex polynomial of $1021. The initial value of the register used for the CRC_B calculation is all ones ($FFFF). When receiving information from the reader, the PICC computes the

CRC on the incoming command, data, and CRC bytes. After the last bit has been processed the CRC register should contain $0000.

In the example illustrated in Figure L-6, the CRC_B is calculated on the “K” bytes of data and then appended to the data. CRC1 is the least significant byte and CRC2 is the most significant byte of the CRC_B. If the CRC_B was calculated as $5A6B, then CRC1 is $6B and CRC2 is $5A.

L.8 Type A Tolerance

The RF Interface is designed for use in multi-protocol applications. It will not latch or lock up if exposed to Type A signals and will not respond to them. The PICC may reset in the presence of Type A field modulation, but is not damaged by exposure to Type A signals.

In a typical multi-protocol application the reader will poll for Type B cards and complete all transactions with any Type B cards present in the field. The reader will then poll for Type A cards and complete all transactions with them. The reader alternates between the two types of modulation and protocols.

Annex M: RF Specifications and Characteristics

The ISO/IEC 10373-6 Test Methods standard contains the test requirements for characterizing ISO/IEC 14443 devices. ISO/IEC 10373-6 utilizes PICCs in the ID-1 credit card size format for all tests. These test methods and the RF signal interface requirements of ISO/IEC 14443 contain PICC and PCD performance requirements that are dependent on the physical size of the PICC antenna.

The ISO/IEC 14443 set of standards do not differentiate PCD and PICC requirements that are PICC antenna size dependent from those that are not. In this Annex all of the RF requirements are summarized, and antenna size related parameters are identified.

M.1 Electrical Characteristics

ISO/IEC 14443 devices, including the CryptoRF family, have their performance specified in terms of the RF interface of the PICC and/or the PCD (Reader). Both components of the RF interface must perform within the specified limits for communications to occur. An ISO/IEC 14443 PICC is not expected to operate with PCDs operating outside the specifications.

M.1.1 AC Characteristics

Table M-1. CryptoRF PICC Characteristics [Not PICC Antenna Size Dependent]

Symbol	Parameter	Min	Nominal	Max	Units	ISO/IEC Spec.
fs	Load Modulation Subcarrier Frequency (fc / 16)	847.06	847.50	847.94	kHz	14443-2 9.2.3
	BPSK Load Modulation Phase Shift		180		degrees	14443-2 9.2.5
ETU	Elementary Time Unit = Bit Time (128 / fc)	9.4346	9.4395	9.4444	uS	14443-2 9.2.1
EGT	Extra Guard Time (PICC to PCD communication)	0		2	ETU	14443-3 7.1.2
ATQB TR0	Guard Time (for ATQB response only)	8		10	ETU	14443-3 7.1.6
TR0	Guard Time (for all other command responses)	8		880	ETU	14443-3 7.1.6
TR1	Synchronization Time	10		11	ETU	14443-3 7.1.6
T_{POR}	Polling Reset Time (no anti-tearing to process)			5	mS	14443-3 5
T_{POR-AT}	Polling Reset Time (anti-tearing write to process)			10	mS	
T_{WR}	Write Cycle Time of EEPROM Memory		1.6	2.0	mS	

The RF Interface characteristics of the CryptoRF family are listed in Table M-1. Compliance with these specifications has been verified by characterization of PICCs with ID-1 size antennas, but these items are not antenna size dependent. The parameters in table M-1 are guaranteed by design. Annex L contains illustrations of the RF interface timing parameters.

M.2 Reader Requirements

Table M-2. ISO/IEC 14443 Reader Requirements [Not PICC Antenna Size Dependent]

Symbol	Parameter	Min	Nominal	Max	Units	ISO/IEC Spec.
fc	Carrier Frequency	13.553	13.560	13.567	Mhz	14443-2 6.1
M.I.	Field Modulation Index (PCD to PICC communication)	8	11	14	percent	14443-2 9.1.2
M.D.	Field Modulation Depth (PCD to PICC communication)	85.2	80.2	75.4	percent	
ETU	Elementary Time Unit = Bit Time (128 / fc)	9.4346	9.4395	9.4444	uS	14443-2 9.1.1
EGT	Extra Guard Time (PCD to PICC communication)	0		57	uS	14443-3 7.1.2
TR2	Frame Delay Time (PICC EOF falling edge to PCD SOF falling edge)	14			ETU	14443-3 7.1.7

The CryptoRF family has been designed to operate with an ISO/IEC 14443 Type B compliant PCDs meeting the requirements listed in Table M-2. CryptoRF has been characterized using PICCs with ID-1 size antennas and ISO/IEC 14443 Type B compliant readers with appropriately sized PCD antennas. The PCD characteristics in table M-2 are not PICC antenna size dependent.

M.3 PICC Antenna Size Dependent Specifications

Table M-3. Antenna Size Dependent Characteristics [ID-1 PICC Antennas Only]

Symbol	Parameter	Min	Nominal	Max	Units	ISO/IEC Spec.
H	Unmodulated Operating Magnetic Field	1.5		7.5	A/m rms	14443-2 6.2
	Maximum Magnetic Field Exposure (Non-Operating)			10	A/m rms	14443-2 4.3.5
	Load Modulation Amplitude at Hmin (1.5 A/m rms)	18.45			mV peak	14443-2 9.2.2 (test per 10373-6)
	Load Modulation Amplitude at Hmin (7.5 A/m rms)	2.68			mV peak	

The specifications in Table M-3 apply to ISO/IEC 14443 PICCs using an ID-1 size antenna only. CryptoRF has been characterized using ID-1 antennas and operates within these limits.

The magnetic field limits of ISO/IEC 14443 are measured using a calibration coil defined in ISO/IEC 10373-6 section 6.1. This calibration coil integrates the field strength over the 3000 mm2 area of a typical ID-1 antenna. The Hmin and Hmax limits of 1.5 and 7.5 A/m rms define the expected operating volume of a PCD with an ID-1 size PICC. The PCD is not allowed to generate a magnetic field strength exceeding 7.5 A/m rms. An ID-1 PICC is required to survive exposure to a 10 A/m rms magnetic field without damage; this non-operating specification guarantees a robust PICC RF interface circuit.

The Load Modulation Amplitude is measured over the full operating magnetic field strength range using an apparatus defined in ISO/IEC 10373-6 section 7.1. This apparatus uses sense coils to detect the signal generated by a PICC transmitting a message to the PCD. The sense coils are optimized to detect a signal generated by an ID-1 PICC. The ISO/IEC 14443 Load Modulation Amplitude requirements apply to this test apparatus only.

M.4 Specifications for Other Antenna Sizes

The specifications in Table M-3 cannot be applied directly to PICCs with larger or smaller antennas. The characteristics in Table M-1 and Table M-2 are applicable to a PICC with any antenna dimensions.

Load Modulation Amplitude measurements on larger or smaller PICCs would require the design and characterization of a new test apparatus. These measurement results would be dependent on the apparatus and cannot be extrapolated from the existing ISO/IEC 14443 specifications.

A reasonable estimate of the Operating Magnetic Field range for a PICC can be made for any PICC antenna size as follows: Determine the area of the PICC antenna by measuring the outside dimensions of the loop antenna. The Magnetic Field strength operating range is inversely proportional to the PICC antenna area (use 3000 mm2 as the ID-1 antenna area). Note however that PCD magnetic field strength must be evaluated with a calibration coil similar in area to the PICC antenna, or the measurement result will not be accurate.

Example 1. Guidelines for operation of a 6000 mm2 PICC Antenna. 3000/6000 = 0.5 The minimum Operating Magnetic Field (Hmin) is 1.5 x 0.5 = 0.75 A/m rms. The maximum Operating Magnetic Field (Hmax) is 7.5 x 0.5 = 3.75 A/m rms. This PICC can be expected to survive exposure to a Non-Operating Magnetic Field of 10 x 0.5 = 5.0 A/m rms.

Example 2. Guidelines for operation of a 1000 mm2 PICC Antenna. 3000/1000 = 3.0 The minimum Operating Magnetic Field (Hmin) is 1.5 x 3.0 = 4.5 A/m rms. The maximum Operating Magnetic Field (Hmax) is 7.5 x 3.0 = 22.5 A/m rms. This PICC can be expected to survive exposure to a Non-Operating Magnetic Field of 10 x 3.0 = 30.0 A/m rms.

Warning: Exposure to magnetic field strengths in excess of 30 A/m rms may be hazardous to your health.

M.5 Modulation Index

The Modulation Index of the PCD generated magnetic field is measured by placing a calibration coil or wire loop near the PCD antenna. Connect this loop to a high impedance oscilloscope probe and measure the amplitude modulation (ASK) waveform as shown in figure M-1. The PCD amplitude Modulation Index is defined in ISO/IEC 14443 part 2 as the M.I. = (A - B) / (A + B). For Type B operation the PCD modulation index is required to be between 8 % and 14 %.

If the PCD modulation is insufficient then the PICC receiver will not successfully decode the transmissions. Excessive modulation reduces the power available to the PICC and may cause it to reset.

Figure M-1. Measurement of the PCD Amplitude Modulation Index

$$\text{Modulation Index} = \frac{(A - B)}{(A + B)}$$

where: A = Unmodulated Signal Amplitude
B = Modulated Signal Amplitude

$$\text{Modulation Depth} = \frac{B}{A}$$

M.6 What is an ID-1 PICC Antenna ?

ISO/IEC 7810 defines the mechanical requirements for plastic identification cards, including smartcards. The nominal ID-1 card dimensions are 85.6 mm by 53.98 mm, and 0.76 mm thick. There are no antenna dimension requirements in ISO/IEC 7810.

Typical antenna dimensions for ID-1 PICCs are described in ISO/IEC 10373-6 section 6.3 as a “Reference PICC” antenna. The outer dimensions of this reference antenna are 72 mm x 42 mm with four concentric turns. The antenna trace width and spacing are both 0.5 mm with a tolerance of +/- 20 %. This is a test antenna, the number of turns required on a real antenna may be more or less than four turns.

Additional guidance regarding ID-1 PICC antenna dimensions is provided in amendment 4 to ISO/IEC 10373-6 in the form of a “Class 1” PICC antenna definition. A “Class 1” PICC has it’s antenna located entirely within a zone defined by two rectangles centered in the ID-1 dimensions. The external rectangle is 81 mm by 49 mm. The internal rectangle is 64 mm x 34 mm, with a 3 mm corner radius. All antenna turns must be located between these rectangles.

Any antenna falling within the “Class 1” dimensions is considered an ID-1 antenna for the purpose of this specification.

M.7 Other Characteristics Impacting Performance

The ISO/IEC 14443 standards do not guarantee that any compliant PCD will operate with any compliant PICC. A reliable RFID system uses PICCs and PCDs matched to the application, with appropriately sized antennas. Discussion of the numerous factors impacting the performance of RFID systems is beyond the scope of this document.

Annex N: Transaction Time

N.1 Command Response Times

The command response time is the time between the end of the frame transmitted by the reader and beginning of the response from the PICC. It consists of the TR0 Guard Time and the TR1 Synchronization Time.

Table N-1. Command Response Timing for the CryptoRF Command Set.

Command	Typical TR0 (microseconds)	Maximum TR0 (microseconds)	Typical TR1 (microseconds)
REQB/WUPB	83	90	97
Slot MARKER	83	90	97
ATTRIB	83	90	97
HLTB	83	90	97
DESELECT	83	90	97
IDLE	83	90	97
Set User Zone	230	235	97
Read User Zone	93	100	97
Write User Zone	1725	2130	97
Write User Zone w/ Anti-Tearing	6690	8300	97
Write User Zone Authentication Mode	112	120	97
Write User Zone Encryption Mode	112	120	97
Write System Zone	1725	2130	97
Write System Zone w/ Anti-Tearing	6690	8300	97
Read System Zone	93	100	97
Verify Crypto	1870	2275	97
Send Checksum	112	120	97
Send Checksum Authentication Mode	1725	2130	97
Send Checksum Encryption Mode	1725	2130	97
Get Checksum	93	100	97
Read Fuse Byte	93	100	97
Write Fuse Byte	1725	2130	97
Check Password	1725	2130	97

N.2 Transaction Times

Typical transaction times for each individual command are listed below. This time includes the command transmission time from the reader, TR0, TR1, and response transmission time from the PICC. The typical transaction times in the table are calculated with zero EGT for both the reader and PICC frames. The maximum transaction times are calculated with EGT = 2 ETUs for both the reader and PICC frames.

Table N-2. Transaction Time for the CryptoRF Command Set.

Command	Typical Transaction Time (milliseconds)	Maximum Transaction Time (milliseconds)
REQB/WUPB	2.4	2.8
Slot MARKER	2.3	2.6
ATTRIB	2.0	2.2
HLTB	1.6	1.8
DESELECT	1.4	1.6
IDLE	1.4	1.6
Set User Zone	1.6	1.8
Read User Zone 1 Byte	1.8	2.0
Read User Zone 16 Bytes	3.2	3.7
Read User Zone 32 Bytes	4.7	5.5
Read User Zone 64 Bytes	7.7	9.2
Write User Zone 1 Byte	3.4	4.1
Write User Zone 8 Bytes	4.1	4.9
Write User Zone w/ AT 8 Bytes	9.0	11.0
Write User Zone 16 Bytes	4.8	5.8
Write User Zone 32 Bytes	6.4	7.6
Read System Zone 1 Byte	1.8	2.0
Read System Zone 16 Bytes	3.2	3.7
Read System Zone 32 Bytes	4.7	5.5
Write System Zone 1 Byte	3.4	4.1
Write System Zone 8 Bytes	4.1	4.9
Write System Zone w/ AT 8 Bytes	9.0	11.0
Write System Zone 16 Bytes	4.8	5.8
Write System Zone 32 Bytes	6.4	7.6
Verify Crypto	4.8	5.7
Send Checksum	1.6	1.8
Send Checksum Authentication Mode	3.2	3.8
Send Checksum Encryption Mode	3.2	3.8
Get Checksum	1.9	2.1
Check Password	3.4	4.1

Annex O: Ordering Information

CryptoRF with 1K bits of User Memory configured as 4 Zones of 32 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC0104CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC0104CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

CryptoRF with 2K bits of User Memory configured as 4 Zones of 64 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC0204CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC0204CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

CryptoRF with 4K bits of User Memory configured as 4 Zones of 128 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC0404CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC0404CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

CryptoRF with 8K bits of User Memory configured as 8 Zones of 128 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC0808CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC0808CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

CryptoRF with 16K bits of User Memory configured as 16 Zones of 128 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC1616CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC1616CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

CryptoRF with 32K bits of User Memory configured as 16 Zones of 256 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC3216CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC3216CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

CryptoRF with 64K bits of User Memory configured as 16 Zones of 512 Bytes each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC6416CRF-MR1	R Module	82 pF	Commercial (0 C to 70 C)
AT88SC6416CRF-WA1	6 mil wafer, 150 mm diameter	82 pF	Industrial (-40 C to 85 C)

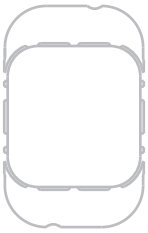
Package Type	Description
R Module	2-lead RF Smart Card Module, XOA2 style, green

The ordering codes for CryptoRF in standard packages are listed here. For additional ordering information see *CryptoRF and Secure RF Standard Product Offerings* at www.atmel.com

O.1 Mechanical

Figure O-1. Mechanical Drawing of Module R Package (XOA2 Style)

Ordering Code: AT88SCxxxxCRF-MR1



Dimension*: 5.06 x 8.00 [mm]
Glob Top: Square - 4.8 x 5.1 [mm]
Thickness: 0.38 [mm]
Pitch: 9.5 mm

Note: *The module dimensions listed refer to the dimensions of the exposed metal contact area. The actual dimensions of the module after excise or punching from the carrier tape are typically 0.4 mm greater in both directions.

Annex P: Errata

P.1 Lot History Code Register Contents

The format of the Lot History Code Register at addresses $10 thru $17 of the Configuration Memory has been changed to contain a Unique Serial Number for each die. The first five bytes of the register contain the Unique Serial Number, while the other three bytes contain additional lot history information. Since this is a read-only register, these five bytes can be used by customers to uniquely identify a particular die for anti-collision, authentication key diversification, or any other purpose required by the application.

Figure P-1. Contents of Lot History Code Register

Addr.	$10	$11	$12	$13	$14	$15	$16	$17	
$10	Unique Serial Number					Other Lot Information			Read Only

This register format change is effective on all CryptoRF products manufactured in July 2008 or later. Prior to July 2008 the contents of the Lot History Code Register are not unique for each die.

Revision History

Doc. Rev.	Date	Comments
5276A	7/2008	Initial document release

Headquarters

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

International

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

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

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

Product Contact

Web Site
www.atmel.com

Technical Support
securerf@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature