AT88RF04C, AT88SC0808CRF, AT88SC1616CRF AT88SC3216CRF, AT88SC6416CRF

CryptoRF EEPROM Memory Full Specification

DATASHEET

Features

- A of a family of devices with user memory of 4 kilobits to 64 kilobits
- Contactless 13.56MHz 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 82pF tuning capacitor
- User EEPROM memory configurations:
  - 64 kilobits configured as sixteen 512 byte (4-Kbit) User Zones [AT88SC6416CRF]
  - 32 kilobits configured as sixteen 256 byte (2-Kbit) User Zones [AT88SC3216CRF]
  - 16 kilobits configured as sixteen 128 byte (1-Kbit) User Zones [AT88SC1616CRF]
  - 8 kilobits configured as eight 128 byte (1-Kbit) User Zones [AT88SC0808CRF]
  - 4 kilobits configured as four 128 byte (1-Kbit) User Zones [AT88RF04C]
  - 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
  - Read-only unique die serial number
- High security features
  - Selectable access rights by zone
  - 64-bit Mutual Authentication Protocol (under license of ELVA)
  - Encrypted checksum
  - Stream encryption using 64-bit key
  - 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

Table of Contents

1. Description . . . 6
2. Introduction . . . 7
   - 2.1 Communications . . . 7
   - 2.2 Scope . . . 7
   - 2.3 Conventions . . . 7
3. User Memory . . . 9
4. Configuration Memory . . . 10
5. Command Set . . . 11
6. Anticollision Command Definitions . . . 12
   - 6.1 REQB/WUPB Polling Commands [$05] . . . 12
   - 6.2 Slot MARKER Command [$s5] . . . 15
   - 6.3 ATTRIB Command [$1D] . . . 17
   - 6.4 HLTB Command [$50] . . . 20
7. Active State Command Definitions . . . 21
   - 7.1 Response Format . . . 21
   - 7.2 Set User Zone Command [$c1] . . . 23
   - 7.3 Read User Zone Command [$c2] . . . 25
   - 7.4 Read User Zone (Large Memory) Command [$c2] . . . 27
   - 7.5 Read User Zone Command with Integrated MAC [$c2] [88RF] . . . 29
   - 7.6 Write User Zone Command [$c3] . . . 32
   - 7.7 Write User Zone (Large Memory) Command [$c3] . . . 35
   - 7.8 Write User Zone Command with Integrated MAC [$c3] [88RF] . . . 38
   - 7.9 Write System Zone Command [$c4] . . . 41
   - 7.10 Write System Zone Command with Integrated MAC [$c4] [88RF] . . . 44
   - 7.11 Write System Zone Command, Write Fuse Byte Option [$c4] . . . 47
   - 7.12 Read System Zone Command [$c6] . . . 50
   - 7.13 Read System Zone Command, Read Fuse Byte Option [$c6] . . . 53
   - 7.14 Read System Zone Command, Read Checksum Option [$c6] . . . 56
   - 7.15 Verify Crypto Command [$c8] . . . 58
   - 7.16 Send Checksum Command [$c9] . . . 60
   - 7.17 DESELECT Command [$cA] . . . 62
   - 7.18 IDLE Command [$cB] . . . 63
   - 7.19 Check Password Command [$cC] . . . 64
8. Transaction Flow . . . 67
9. Absolute Maximum Ratings . . . 68
10. Reliability . . . 68
11. Electrical Characteristics . . . 69
   - 11.1 Tamper Detection . . . 69

Appendix A. Terms and Abbreviations 70

Appendix B. Standards and Reference Documents 75
B.1 International Standards 75
B.2 References 75

Appendix C. User Memory Maps. 76

Appendix D. Configuration Memory Maps 82

Appendix E. Device Personalization. 86
E.1 User Memory Initialization 87
E.2 Polling Response and OTP Memory Personalization 87
E.3 Transport Password Check 88
E.4 Security Fuse Programming 89
E.5 Secure Personalization 89

Appendix F. Secure Personalization [88RF] 90
F.1 User Memory Initialization 91
F.2 Transport Password Check 91
F.3 Security Fuse Programming 91
F.4 Secure Personalization Mode Data Encryption 91

Appendix G. Security Fuses 93
G.1 Reading the Security Fuses 93
G.2 Programming the Fuse Bits 93
G.3 Configuration Memory Access Control 94

Appendix H. Configuration of Password and Access Control Registers . 96
H.1 User Zone Configuration Options 96
H.2 Access Registers (AR) [88RF] 98
H.3 Device Configuration Options 101

Appendix I. Using Password Security 103
I.1 Communication Security 103
I.2 Transport Password 103
I.3 The Password and PAC Registers 104
I.4 Password Security Options 105
I.5 Password Verification 106
I.6 Changing Passwords 107
I.7 Supervisor Password 107

Appendix J. Using Authentication Communication Security. 108
J.1 Communication Security 108
J.2 Authentication Security Options [88SC] 108
J.3 Authentication Security Options [88RF] 109
J.4 The Password Register [88SC] 110
J.5 The Key Register [88RF] 111
J.6 Key Sets 112
J.7 AAC Registers 113
J.8 Authentication Activation 114
J.9 Set User Zone and Checksums 116
J.10 Passwords 116
J.11 Deactivating Authentication Communication Security 116

Appendix K. Using Encryption Communication Security 117
K.1 Communication Security 117
K.2 Encryption Security Options [88SC] 117
K.3 Encryption Security Options [88RF] 118
K.4 The Password Register [88SC] 119
K.5 The Key Register [88RF] 120
K.6 Key Sets 121
K.7 AAC Registers 122
K.8 Encryption Activation 124
K.9 Set User Zone and Checksums 126
K.10 Passwords 126
K.11 Deactivating Encryption Communication Security 126

Appendix L. Understanding Anti-Tearing 127
L.1 Tearing Explained 127
L.2 CryptoRF Anti-Tearing 127
L.3 Performance Impact of Anti-Tearing 129
L.4 Reliability Impact of Anti-Tearing 129
L.5 Activating Anti-Tearing 130

Appendix M. Personalization of the Anticollision Registers 131
M.1 Anticollision Procedure 131
M.2 Anticollision Registers 131
M.3 Summary 135

Appendix N. Understanding Anticollision 136

Appendix O. The ISO/IEC 14443 Type B RF Signal Interface 138
O.1 RF Signal Interface 138
O.2 Data Format 138
O.3 Frame Format 139
O.4 Reader Data Transmission 139
O.5 Card Data Transmission 140
O.6 Response Timing 140
O.7 CRC Error Detection 141
O.8 Type A Tolerance 141

Appendix P. RF Specifications and Characteristics 142
P.1 Electrical Characteristics 142
P.2 Reader Requirements 143
P.3 PICC Antenna Size Dependent Specifications 143
P.4 Specifications for Other Antenna Sizes 144
P.5 Modulation Index 144
P.6 What is an ID-1 PICC Antenna? 145
P.7 Other Characteristics Impacting Performance 145

Appendix Q. Transaction Time 146
Q.1 Command Response Times [88SC] 146
Q.2 Command Response Times [88RF] 147
Q.3 Transaction Times [88SC] 148
Q.4 Transaction Times [88RF] 149

Appendix R. 88RF PICC Backward Compatibility 150
R.1 Error Handling 150
R.2 Security Options 150
R.3 Attempt Counters 150
R.4 Checksums 150
R.5 Personalization 151

Appendix S. Ordering Information 152
S.1 CryptoRF with 4Kb of User Memory Configured as 4 Zones of 128 bytes Each 152
S.2 CryptoRF with 8Kb of User Memory Configured as 8 Zones of 128 bytes Each 152
S.3 CryptoRF with 16Kb of User Memory Configured as 16 Zones of 128 bytes Each 152
S.4 CryptoRF with 32Kb of User Memory Configured as 16 Zones of 256 bytes Each 153
S.5 CryptoRF with 64Kb of User Memory Configured as 16 Zones of 512 bytes Each 153
S.6 Package Types 153
S.7 Packaging Information — Mechanical Drawings 154

Appendix T. Errata 157
T.1 Lot History Code Register Contents 157
T.2 Read User Zone command 157
T.3 Read User Zone command PARAM Codes [88RF] 157
T.4 Status Codes [88RF] 157
T.5 Encryption Activation Change [88RF] 158

Appendix U. Revision History 159

1. Description

The Atmel® CryptoRF® family integrates a 13.56MHz RF interface with Atmel 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.

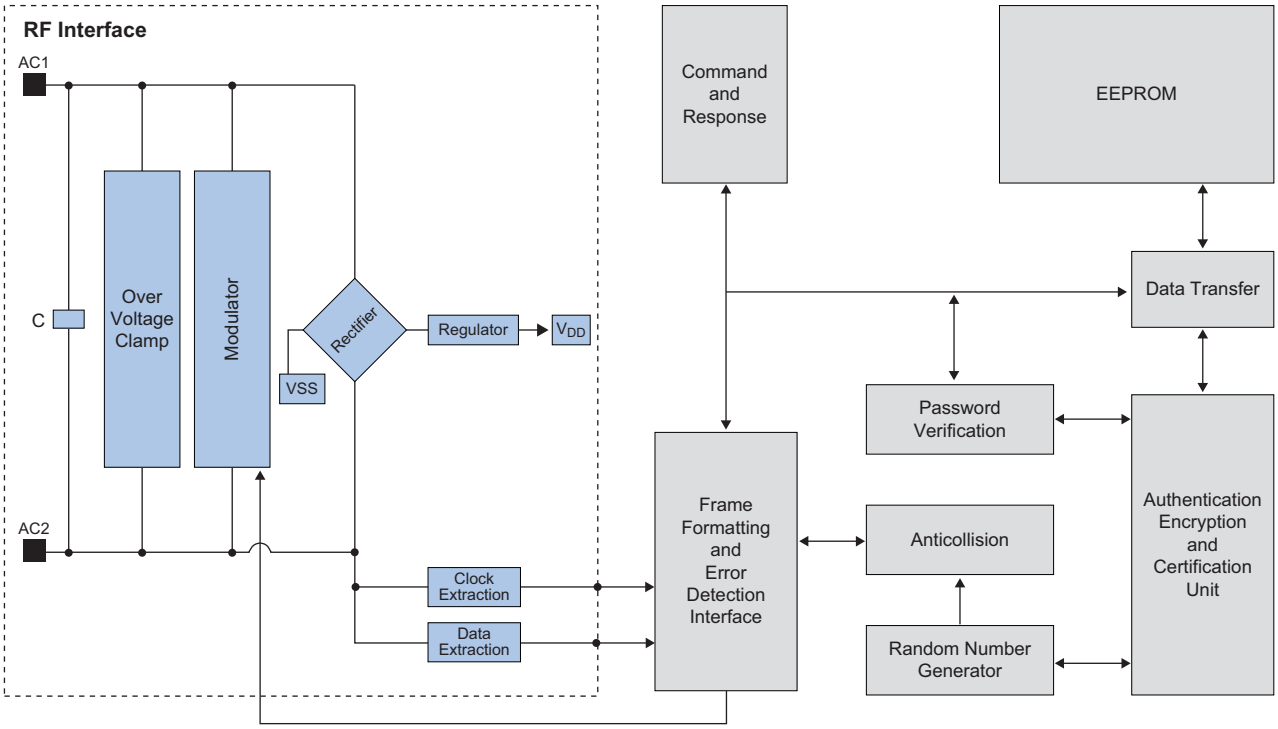
For communications, the RF interface utilizes the ISO/IEC 14443-2 and -3 Type B bit timing and signal modulation schemes, and the ISO/IEC 14443-3 Slot-MARKER Anticollision Protocol. Data is exchanged half duplex at a 106-kbit per second rate, with a two byte CRC_B providing error detection capability.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

The five products in the CryptoRF family contain 4 to 64 kilobits of user memory plus two kilobits of configuration memory. The two kilobits of configuration memory contains:

- Read/Write password sets
- Four crypto key sets
- Security access registers for each user zone
- Password/Key registers for each zone

The CryptoRF command set is optimized for a multi-card 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.

Figure 1-1. Block Diagram



2. Introduction

The CryptoRF family consists of devices in the AT88SCxxCRF and AT88RFxxC catalog number series. The first generation devices are assigned catalog numbers in the AT88SCxxCRF series. The second generation devices are assigned catalog numbers in the AT88RFxxC series. Several security options have been added to the second generation devices to enhance system security.

2.1 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.

2.2 Scope

This *CryptoRF Specification* document includes all specifications for the Normal, Authentication, and Encryption modes of CryptoRF operation.

2.3 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 Appendix A “Terms and Abbreviations” on page 70.

Table 2-1. Terms

Abbrev.	Term	Definition
PCD	Proximity Coupling Device	The reader/writer and antenna.
PICC	Proximity Integrated Circuit Card	The tag/card containing the IC and antenna.
RFU	Reserved for Future Use	Any feature, memory location, or bit that is held as reserved for future use.
$ 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).
88SC		CryptoRF devices in the AT88SCxxCRF catalog number series.
88RF		CryptoRF devices in the AT88RFxxC catalog number series.

This document contains the specifications for AT88SCxxCRF and AT88RFxxC CryptoRF devices. Any specification that applies only to the first generation AT88SCxxCRF devices references: 88SC devices, 88SC PICCs, or contain [88SC] in the section title. Any specification that applies only to the second generation AT88RFxxC devices references: 88RF devices, 88RF PICCs, or contain [88RF] in the section title. Specifications that apply to all devices are referred to as CryptoRF specifications.

Each command/response exchange between the PCD and PICC is formatted as shown in Figure 2-1. 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 2-1, 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 2-1. Example Command and Response Format

	Reader		PICC	
Command First Byte >	$1D			
Command Second Byte >	$00			
Command Third Byte >	ADDR			
Command Fourth Byte >	$F	XX		
Command Fifth Byte >	$51			
CRC First Byte >	CRC1			
CRC Second Byte >	CRC2			
TR2				
Response First Byte >			$0	CID
Response Second Byte >			DATA	
CRC First Byte >			CRC1	
CRC Second Byte >			CRC2	

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.

3. User Memory

The User EEPROM Memory characteristics are summarized in 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. See Appendix C “User Memory Maps” on page 76.

Table 3-1. CryptoRF User Memory Characteristics

CryptoRF Part Number	User Memory Size		User Memory Organization		Write Characteristics	
	Bits	Bytes	# of Zones	Bytes/Zones	Standard Write	Anti-Tearing Write
AT88RF04C	4K	512K	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

4. 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. See Appendix D “Configuration Memory Maps” on page 82.

Table 4-1. Configuration Memory Characteristics

CryptoRF Part Number	Password Sets	Key Sets	OTP Memory	Transport Password	
			Free For Customer Use	PW Index	Password
AT88RF04C	4	4	25 bytes	$07	$30 1D D2
AT88SC0808CRF	8	4	27 bytes	$07	$40 7F AB
AT88SC1616CRF	8	4	27 bytes	$07	$50 44 72
AT88SC3216CRF	8	4	27 bytes	$07	$60 78 AF
AT88SC6416CRF	8	4	27 bytes	$07	$70 BA 2E

5. Command Set

The CryptoRF command set contains two types of commands:

- **Anticollision Commands** — Explicitly defined in ISO/IEC 14443-3:2001.
- **Active State Commands** — Atmel defined commands that are compliant with the ISO/IEC 14443-3:2001 requirements. These 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 5-1. 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	Hexadecimal
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 5-2. 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	Hexadecimal
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.									

6. Anticollision Command Definitions

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

6.1 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
		APP1	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	

6.1.1 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.

6.1.2 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 6-1 describes the AFI matching criteria. An AFI of $00 activates all Type B PICCs.

Table 6-1. 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.

Notes: 1. “Y” = $1 to $F
2. “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 6-1. Definition 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 6-2. 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	0	RFU
1	1	1	RFU

Table 6-3. Coding of the REQB/WUPB Selection Bit in the PARAM Byte.

Bit 3	Command
0	REQB
1	WUPB

CRC: Communication error detection bytes.

6.1.3 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 6-4.

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

Device Number	Density Code
AT88RF04C	$22
AT88SC0808CRF	$33
AT88SC1616CRF	$44
AT88SC3216CRF	$54
AT88SC6416CRF	$64

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

CRC: Communication error detection bytes.

6.1.4 Error Handling

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

6.1.5 Notes

The REQB and WUPB commands are identical for 88SC and 88RF CryptoRF PICCs.

6.2 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
		APP1 — 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

6.2.1 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 one is issued, and the ATQB response (if any) is received, the PCD will transmit Slot MARKER commands with slot values “S” of two to “N” to define the start of each timeslot for anticollision. 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.

6.2.2 Command Field Description

S: The slot number “S” is encoded within the command byte as shown in Table 6-5.

CRC: Communication error detection bytes.

Table 6-5. 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

6.2.3 Response Field Description

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.

6.2.4 Error Handling

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

6.2.5 Notes

The Slot MARKER command is identical for 88SC and 88RF CryptoRF PICCs.

6.3 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
			CRC1	
			CRC2	

SUCCESS RESPONSE

6.3.1 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.

6.3.2 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 one, two, and three do not alter the behavior of CryptoRF PICCs.

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 four and in the ATTRIB Response is encoded as shown in Table 6-6 and Table 6-7. 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 6-6. Coding of the Card ID in the ATTRIB Command and Response for 88SC PICCs.

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	0	1	13
1	1	1	0	14
1	1	1	1	Not Supported

Table 6-7. Coding of the Card ID in the ATTRIB Command and Response for 88RF PICCs.

Bit 7	Bit 6	Bit 5	Bit 4	CID
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	1	1	13
1	1	1	0	14
1	1	1	1	Not Supported

CRC: Communication error detection bytes.

6.3.3 Response Field Descriptions

CID: The PICC transmits its assigned card ID in the response.

CRC: Communication error detection bytes.

6.3.4 Error Handling

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

6.3.5 Notes

The ATTRIB command for 88SC PICCs is used to assign a CID in the range of 1 to 15 to the PICC; CID = 0 is not supported. The ATTRIB command for 88RF PICCs is used to assign a CID in the range of 0 to 15 to the PICC.

6.4 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	

6.4.1 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.

6.4.2 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.

6.4.3 Response Field Description

CRC: Communication error detection bytes.

6.4.4 Error Handling

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

6.4.5 Notes

The HLTB command is identical for 88SC and 88RF CryptoRF PICCs.

7. Active State Command Definitions

Commands in this section are arranged in order by the hexadecimal code in the command byte. Several of the Active state commands perform multiple functions; the value of the PARAM byte determines which function is performed.

Table 7-1. 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	Hexadecimal
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.									

7.1 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 7-2. 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 PICC information.
Password Attempts Count				0	0	0	1	NACK, Check Password Attempt Failure.
Auth. Attempts Count				0	0	0	1	NACK, Authentication or Encryption Attempt Failure.

The ACK/NACK byte reports success or failure of the command execution. In the event of a Check Password command failure or Verify Crypto command failure the ACK/NACK byte contains an attempts count coded as shown in Table 7-3 and Table 7-4.

The STATUS byte provides information to the host application indicating the state of the PICC or the reason for failure of a requested operation. The STATUS byte does not report the success or failure of a command. In the event of multiple errors, the STATUS byte reports the first error detected.

The PICC ignores commands that do not have a matching CID. Invalid command codes are also ignored.

Table 7-3. Coding of the Password Attempts Count or Authentication Attempts Count in the 88SC ACK/NACK Byte.

Hexadecimal	Bit 7	Bit 6	Bit 5	Bit 4	Description
$0	0	0	0	0	No Failed Attempts
$1	0	0	0	1	1 Failed Attempt
$2	0	0	1	0	2 Failed Attempts
$3	0	0	1	1	3 Failed Attempts
$4	0	1	0	0	4 Failed Attempts
$5	0	1	0	1	5 Failed Attempts
$6	0	1	1	0	6 Failed Attempts
$7	0	1	1	1	7 Failed Attempts
$8	1	0	0	0	8 Failed Attempts

Table 7-4. Coding of the Password Attempt Count or Authentication Attempts Count in the 88RF ACK/NACK Byte.

Hexadecimal	Bit 7	Bit 6	Bit 5	Bit 4	Description
$0	0	0	0	0	No Failed Attempts
$1	0	0	0	1	1 Failed Attempt
$2	0	0	1	0	2 Failed Attempts
$3	0	0	1	1	3 Failed Attempts
$4	0	1	0	0	4 Failed Attempts
$5	0	1	0	1	5 Failed Attempts
$6	0	1	1	0	6 Failed Attempts
$7	0	1	1	1	7 Failed Attempts
$8	1	0	0	0	8 Failed Attempts
$9	1	0	0	1	9 Failed Attempts
$A	1	0	1	0	10 Failed Attempts
$B	1	0	1	1	11 Failed Attempts
$C	1	1	0	0	12 Failed Attempts
$D	1	1	0	1	13 Failed Attempts
$E	1	1	1	0	14 Failed Attempts
$F	1	1	1	1	15 Failed Attempts (LOCK)

7.2 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 Response >		CID, $1 ACK/NACK STATUS CRC1 CRC2

7.2.1 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 is active for the selected 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.

7.2.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

PARAM: Selects the User Zone and sets anti-tearing on or off.

Table 7-5. Definition 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 7-6. Coding of the Anti-Tearing Select Bit within the PARAM Byte

Bit 7	Write User Zone
0	Normal Write Enabled
1	Anti-Tearing Write Enabled

Table 7-7. 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.

7.2.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.2.4 Error Handling

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

Table 7-8. 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

7.2.5 Notes

The Set User Zone command is identical for 88SC and 88RF CryptoRF PICCs.

7.3 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
PARAM = $00 >	PARAM	
	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		

7.3.1 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. Reading beyond the end of the current User Zone is prohibited. Only PICCs in the Active State are permitted to answer this command.

If Encryption Communication Security is active the DATA bytes are encrypted; no other bytes are encrypted. In the Normal and Authentication Communication Security modes none of the bytes are encrypted.

7.3.2 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. PARAM = $00 selects the normal Read User Zone command.

ADDR: The starting address of the data to read.

L: The number of bytes to read minus one. 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.

7.3.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.3.4 Error Handling

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

Table 7-9. 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
PARAM Invalid	$A1	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

7.3.5 Notes

The Read User Zone command is identical for 88SC and 88RF CryptoRF PICCs when PARAM = $00.

7.4 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	
PARAM = ADDR H	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		

7.4.1 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. Reading beyond the end of the current User Zone is prohibited. Only PICCs in the Active State are permitted to answer this command.

If Encryption Communication Security is active the DATA bytes are encrypted; no other bytes are encrypted. In the Normal and Authentication Communication Security modes none of the bytes are encrypted.

7.4.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte is the ADDR H byte of Read User Zone (Large Memory) command.

Table 7-10. Definition of the PARAM (ADDR H) Byte of the Read 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

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

L: The number of bytes to read minus one. 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.

7.4.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.4.4 Error Handling

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

Table 7-11. Status Codes Returned in the Read User Zone (Large Memory) Response.

Error/Status Message	Status Code	Type
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

7.4.5 Notes

The Read User Zone (Large Memory) command is not supported by 88RF PICCs.

7.5 Read User Zone Command with Integrated MAC [$c2] [88RF]

The Read User Zone command with Integrated MAC reads data from the currently selected User Zone on 88RF PICCs. This command can only be used when the Authentication or Encryption Communication Security mode is active.

	Reader	PICC	
Command >	CID	$2	
PARAM = $80 >	PARAM		
	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”		
	MAC1		< Checksum
	MAC2		
	STATUS		< Status Code
	CRC1		
	CRC2		

7.5.1 Operation

The Read User Zone command with Integrated MAC reads data from the 88RF device's currently selected User Zone and also returns the cryptographic checksum. If the RCS bit of the DCR register is set to 1b, then the cryptographic engine is reset after the checksum is read. If the RCS bit of the DCR register is set to 0b, then the cryptographic engine is not reset by this command.

The data byte address is internally incremented as each byte is read from memory. Reading beyond the end of the current User Zone is prohibited. Only PICCs in the Active State are permitted to answer this command. If the Authentication or Encryption Communication Security mode is not active, then a NACK response is returned.

If the Encryption Communication Security mode is active, then the DATA bytes are encrypted. In Authentication Communication Security mode the DATA bytes are not encrypted.

7.5.2 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 7-12. PARAM Byte Options for the Read User Zone Command for 88RF PICCs.

Command	PARAM
Read User Zone (Normal/Legacy)	$00
Read User Zone with Integrated MAC	$80
All Other Values Are Not Supported.	

ADDR: The starting address of the data to read.

L: The number of bytes to read minus one. 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.

7.5.3 Response Field Descriptions

CID: The PICC transmits its 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.

MAC: The checksum bytes read from the cryptographic engine.

STATUS: PICC status code.

CRC: Communication error detection bytes.

7.5.4 Error Handling

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

Table 7-13. 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
PARAM Invalid	$A1	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

7.5.5 Notes

The Read User Zone command with Integrated MAC is not supported by 88SC PICCs.

7.6 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	
PARAM =$00 >	PARAM	
	ADDR	
	“L”	
	DATA 1	
	DATA 2	
	…….	
	DATA “L”	
	DATA “L+1”	
	CRC1	
	CRC2	

Echo Command >	CID	$3
	ACK/NACK	
	STATUS	
	CRC1	
	CRC2	

7.6.1 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.

If Encryption Communication Security is active the DATA bytes are encrypted; no other bytes are encrypted. In the Normal and Authentication Communication Security modes none of the bytes are encrypted.

The Write User Zone command includes an automatic data verification function when used on 88RF PICCs. After the EEPROM write is complete the data verification logic reads the new EEPROM contents and compares it to the data received in the Write User Zone command. If the data does not match then the PICC returns a NACK response with $ED in the status byte. If the data matches, the PICC returns an ACK response.

7.6.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte selects the type of write operation to be performed. PARAM = $00 selects the normal Write User Zone command.

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

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

Table 7-14. Write Characteristics of CryptoRF

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88RF04C	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 user memory.

CRC: Communication error detection bytes.

7.6.3 Response Field Description

CID: The PICC transmits its 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.

7.6.4 Error Handling

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

Table 7-15. 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
PARAM Invalid	$A1	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
Checksum Failure	$C9	NACK
Password Required	$D9	NACK
Modify Forbidden	$E9	NACK
Memory Write Error - Data Mismatch	$ED	NACK
Memory Access Error	$EE	ACK/NACK

7.6.5 Notes

The Write User Zone command is identical for 88SC and 88RF CryptoRF PICCs when PARAM = $00. Automatic data write verification is performed by 88RF PICCs; this function is not supported by 88SC PICCs.

7.7 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	
PARAM = ADDR H	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	

7.7.1 Operation

The Write User Zone (Large Memory) command operates identically to the normal 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.

If Encryption Communication Security is active the DATA bytes are encrypted; no other bytes are encrypted. In the Normal and Authentication Communication Security modes none of the bytes are encrypted.

7.7.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte is the ADDR H byte of Write User Zone (Large Memory) command.

Table 7-16. Definition of the PARAM (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

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

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

Table 7-17. 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.

7.7.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.7.4 Error Handling

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

Table 7-18. 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

7.7.5 Notes

The Write User Zone (Large Memory) command is not supported by 88RF PICCs.

7.8 Write User Zone Command with Integrated MAC [$c3] [88RF]

The Write User Zone command with Integrated MAC writes data into the currently selected User Zone of 88RF PICCs. This command can only be used when the Authentication or Encryption Communication Security mode is active.

	Reader		PICC
Command >	CID	$3	
PARAM = $80 >	PARAM		
	ADDR		
	“L”		
	DATA 1		
	DATA 2		
	…….		
	DATA “L”		
	DATA “L+1”		
Checksum >	MAC1		
	MAC2		
	CRC1		
	CRC2		

Echo Command >	CID	$3
	ACK/NACK	
	STATUS	
	CRC1	
	CRC2	

7.8.1 Operation

The Write User Zone command with Integrated MAC writes data in the 88RF 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. If the Authentication or Encryption Communication Security mode is not active, then a NACK response is returned. If the checksum does not match, then a NACK response is returned, the write operation is aborted, and the cryptographic engine is reset.

The Write User Zone command with Integrated MAC includes an automatic data verification function. After the EEPROM write is complete the data verification logic reads the new EEPROM contents and compares it to the data received in the Write User Zone command. If the data does not match the PICC returns a NACK response with $ED in the status byte. If the data matches, the PICC returns an ACK response.

If the Encryption Communication Security mode is active, then the DATA bytes are encrypted. In Authentication Communication Security mode the DATA bytes are not encrypted.

7.8.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

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

Table 7-19. PARAM Byte Options for the Write User Zone Command for 88RF PICCs.

Command	PARAM
Write User Zone (Normal / Legacy)	$00
Write User Zone with Integrated MAC	$80
All Other Values Are Not Supported.	

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

L: The number of bytes to write minus one. “L” cannot exceed the 16 byte physical page size of the memory. In Anti-Tearing mode, the maximum number of bytes that can be written is eight bytes.

Table 7-20. Write Characteristics of 88RF PICCs

CryptoRF Part Number	Write Characteristics	
	Normal Write	Anti-Tearing Write
AT88RF04C	1 to 16 bytes	1 to 8 bytes

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

MAC: The checksum bytes sent to the cryptographic engine.

CRC: Communication error detection bytes.

7.8.3 Response Field Description

CID: The PICC transmits its 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.

7.8.4 Error Handling

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

Table 7-21. 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
Access Denied (User Zone Not Set)	$99	NACK
Access Denied (Security Fuses Invalid)	$99	NACK
PARAM Invalid	$A1	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Authentication or Encryption Activation Required	$A9	NACK
Data Written (Program Only Mode)	$B0	ACK
Checksum Failure	$C9	NACK
Password Required	$D9	NACK
Modify Forbidden	$E9	NACK
Memory Write Error — Data Mismatch	$ED	NACK
Memory Access Error	$EE	ACK/NACK

7.8.5 Notes

The Write User Zone command with Integrated MAC is not supported by 88SC PICCs.

7.9 Write System Zone Command [$c4]

The Write System Zone command writes data to the configuration memory.

	Reader	PICC
Command >	CID, $4	
PARAM = $00 >	PARAM	
	ADDR	
	"L"	
	DATA 1	
	DATA 2	
	…….	
	DATA "L"	
	DATA "L+1"	
	CRC1	
	CRC2	

Echo Command >	CID, $4	
	ACK/NACK	
	STATUS	
	CRC1	
	CRC2	

7.9.1 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.

If Authentication or Encryption Communication Security is active the DATA bytes written to the password (PW) registers are encrypted; no other bytes are encrypted. In the Normal Communication Security mode none of the bytes are encrypted.

The Write System Zone command includes an automatic data verification function when used on 88RF PICCs. After the EEPROM write is complete the data verification logic reads the new EEPROM contents and compares it to the data received in the Write System Zone command. If the data does not match then the PICC returns a NACK response with $ED in the status byte. If the data matches, the PICC returns an ACK response.

7.9.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte selects the type of write operation to be performed. 88RF PICCs do not support anti-tearing writes to the configuration memory.

Table 7-22. 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 byte
All Other Values Are Not Supported.				

ADDR: The starting address of the data to write.

L: The number of bytes to read minus one. L cannot exceed the physical page size of the memory. In Anti-Tearing mode, the maximum number of bytes that can be written is eight bytes.

Table 7-23. Write Characteristics of CryptoRF Configuration Memory

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88RF04C	1 to 16 bytes	Not Supported
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.

CRC: Communication error detection bytes.

7.9.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.9.4 Error Handling

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

Table 7-24. 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
Integrated Checksum Mode Write Complete	$B0	ACK
Access denied (Write Not Allowed)	$BA	NACK
Checksum Failure	$C9	NACK
Password Required	$D9	NACK
Memory Write Error — Data Mismatch	$ED	NACK
Memory Access Error	$EE	ACK/NACK

7.9.5 Notes

The Write System Zone command is identical for 88SC and 88RF CryptoRF PICCs when PARAM = $00. 88RF PICCs do not support PARAM = $80. Automatic data write verification is performed by 88RF PICCs; this function is not supported by 88SC PICCs.

7.10 Write System Zone Command with Integrated MAC [$c4] [88RF]

The Write System Zone command with Integrated MAC writes data to the 88RF PICC configuration memory. This command can only be used when the Encryption Communication mode is active. This command is only available when the Security fuses are: SEC = 0b, ENC = 0b, SKY = 1b, PER = 1b.

	Reader	PICC
Command >	CID	$4
	PARAM	
	ADDR	
	“L”	
	DATA 1	
	DATA 2	
	…….	
	DATA “L”	
	DATA “L+1”	
Checksum >	MAC1	
	MAC2	
	CRC1	
	CRC2	

Echo Command >	CID	$4
	ACK/NACK	
	STATUS	
	CRC1	
	CRC2	

7.10.1 Operation

The Write System Zone command with Integrated MAC writes data into the 88RF PICC 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. If the Encryption Communication mode is not active, then a NACK response is returned. If the checksum does not match, then a NACK response is returned, the write operation is aborted, and the cryptographic engine is reset.

The Write System Zone command with Integrated MAC includes an automatic data verification function. After the EEPROM write is complete the data verification logic reads the new EEPROM contents and compares it to the data received in the Write System Zone command. If the data does not match the PICC returns a NACK response with $ED in the status byte. If the data matches, the PICC returns an ACK response.

7.10.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

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

Table 7-25. PARAM Byte Options for the Write System Zone Command for 88RF PICCs

Command	PARAM	ADDR	"L"	DATA
Write System Zone (Normal / Legacy)	$00	Address	# of bytes – 1	"L + 1" bytes
Write Fuse Byte	$01	Fuse addr	$00	1 byte
Write System Zone with Integrated MAC	$08	Address	# of bytes – 1	"L + 1 bytes"
All Other Values Are Not Supported.				

ADDR: The starting address of the data to write.

L: The number of bytes to write minus one. L cannot exceed the 16 byte physical page size of the memory.

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

MAC: The checksum bytes sent to the cryptographic engine.

CRC: Communication error detection bytes.

7.10.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.10.4 Error Handling

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

Table 7-26. Status Codes Returned in the Write System Zone with Integrated MAC Response

Error/Status Message	Status Code	Type
No errors	$00	ACK
PARAM Invalid	$A1	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Integrated Checksum Mode Write Complete	$B0	ACK
Access denied (Write Not Allowed)	$BA	NACK
Checksum Failure	$C9	NACK
Password Required	$D9	NACK
Memory Write Error - Data Mismatch	$ED	NACK
Memory Access Error	$EE	ACK/NACK

7.10.5 Notes

The Write System Zone command with Integrated MAC is not supported by 88SC PICCs.

7.11 Write System Zone Command, Write Fuse Byte Option [$c4]

The Write Fuse Byte Option of the Write System Zone command is used to program the security fuses.

	Reader	PICC
Command >	CID, $4	
PARAM = $01 >	PARAM	
	ADDR	
L = $00 >	"L"	
	DATA 1	
	CRC1	
	CRC2	
Echo Command >		CID, $4
		ACK/NACK
		STATUS
		CRC1
		CRC2

7.11.1 Operation

The Write Fuse Byte Option of the Write System Zone command programs the security fuses. Once programmed, the fuses cannot be erased. This operation can be performed in the Normal, Authentication, or Encryption Communication modes. The fuse byte value is never encrypted. Only PICCs in the Active State are permitted to answer this command.

7.11.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

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

Table 7-27. 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 byte
All Other Values Are Not Supported				

ADDR: 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.

Table 7-28. Coding of ADDR for 88SC PICC Fuse Programming

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

Table 7-29. Coding of ADDR for 88RF PICC Fuse Programming

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	ENC
$04	0	0	0	0	0	1	0	0	SKY
$00	0	0	0	0	0	0	0	0	PER

L: The number of bytes to write minus one. L must be $00 when writing the Fuse Bytes.

DATA: 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.

7.11.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.11.4 Error Handling

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

Table 7-30. Status Codes Returned in the Write System Zone Response for Fuse Byte Writes

Error/Status Message	Status Code	Type
Fuse Byte (Successful Fuse Byte Write)	Fuse byte	ACK
Fuse Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Password Required	$D9	NACK
Fuse Access Denied	$DF	NACK
Access denied (Fuse Order Incorrect)	$E9	NACK
Memory Access Error	$EE	ACK/NACK

7.11.5 Notes

The Write Fuse Byte option of the Write System Zone command is identical for 88SC and 88RF CryptoRF PICCs.

7.12 Read System Zone Command [$c6]

The System Read command allows reading of system data from the configuration memory.

	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

7.12.1 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. Only PICCs in the Active State are permitted to answer this command.

If Authentication or Encryption Communication Security is active the DATA bytes read from the password (PW) registers are encrypted; no other bytes are encrypted. In the Normal Communication Security mode none of the bytes are encrypted.

7.12.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

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

Table 7-31. 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 one. 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.

7.12.3 Response Field Descriptions

CID: The PICC transmits its 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".

ACK: Acknowledge, the command executed correctly.

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

STATUS: PICC status code.

CRC: Communication error detection bytes.

7.12.4 Error Handling

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

Table 7-32. 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

7.12.5 Notes

The Read System Zone command is identical for 88SC and 88RF CryptoRF PICCs.

7.13 Read System Zone Command, Read Fuse Byte Option [$c6]

The Read Fuse Byte Option of the Read System Zone command reads the security fuse byte.

	Reader	PICC
Command >	CID, $6	
PARAM = $01 >	PARAM	
ADDR = $FF >	ADDR	
L = $00 >	"L"	
	CRC1	
	CRC2	

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

Echo Command >	CID	$6	SUCCESS RESPONSE
	ACK		
	DATA 1		< Fuse Byte
	STATUS		<Status Code
	CRC1		
	CRC2		

7.13.1 Operation

The Read Fuse Byte Option of the Read System Zone command reads the Security Fuse byte. This operation can be performed in the Normal, Authentication, or Encryption Communication modes. The fuse byte value is never encrypted. Only PICCs in the Active State are permitted to answer this command.

7.13.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte selects the type of read operation to be performed. PARAM must be $01 for Read Fuse Byte.

Table 7-33. 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 address must be $FF for Read Fuse Byte.

L: The number of bytes to read minus one. L must be $00 for Read Fuse Byte.

CRC: Communication error detection bytes.

7.13.3 Response Field Descriptions

CID: The PICC transmits its assigned card ID in the response.

DATA: The Security Fuse Byte value.

Figure 7-1. Definition of the DATA Byte Received When Reading the Fuse Byte of 88SC PICCs

F7	F6	F5	F4	F3	F2	F1	F0	
RFU	RFU	RFU	RFU	SEC	PER	CMA	FAB	
X	X	X	X	0	1	1	1	Default Value

Figure 7-2. Coding of the DATA Byte Received When Reading the Fuse Byte of 88RF PICCs

F7	F6	F5	F4	F3	F2	F1	F0	
RFU	RFU	RFU	RFU	SEC	ENC	SKY	FAB	
X	X	X	X	0	1	1	1	Default Value

ACK: Acknowledge, the command executed correctly.

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

STATUS: PICC status code.

CRC: Communication error detection bytes.

7.13.4 Error Handling

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

Table 7-34. Status Codes Returned in the Read System Zone Response When Reading the Fuse Byte.

Error/Status Message	Status Code	Type
No errors	$00	ACK
PARAM Invalid	$A1	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Memory Access Error	$EE	ACK/NACK

7.13.5 Notes

The Read Fuse Byte Option of the Read System Zone command is identical for 88SC and 88RF CryptoRF PICCs.

7.14 Read System Zone Command, Read Checksum Option [$c6]

The Read Checksum Option of the System Read command reads the checksum from the cryptographic engine.

	Reader	PICC

Command >	CID	$6
PARAM = $02 >	PARAM	
ADDR = $FF >	ADDR	
L = $01 >	“L”	
	CRC1	
	CRC2	

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

Echo Command >	CID	$6	SUCCESS RESPONSE
	ACK		
	DATA 1		< MAC1
	DATA 2		< MAC2
	STATUS		<Status Code
	CRC1		
	CRC2		

7.14.1 Operation

The Read Checksum Option of the Read System Zone command reads the checksum from the cryptographic engine. This operation can be performed in the Normal, Authentication, or Encryption Communication modes. Only PICCs in the Active State are permitted to answer this command.

7.14.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

PARAM: The PARAM byte selects the type of read operation to be performed. PARAM must be $02 for Read Checksum.

Table 7-35. 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 address must be $FF for Read Checksum.

L: The number of bytes to read minus one. L must be $01 for Read Checksum.

CRC: Communication error detection bytes.

7.14.3 Response Field Descriptions

CID: The PICC transmits its assigned card ID in the response.

DATA: The two checksum bytes read from the cryptographic engine.

ACK: Acknowledge, the command executed correctly.

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

STATUS: PICC status code.

CRC: Communication error detection bytes.

7.14.4 Error Handling

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

Table 7-36. Status Codes returned in the Read System Zone response for Read Checksum.

Error/Status Message	Status Code	Type
No errors	$00	ACK
PARAM Invalid	$A1	NACK
Address Invalid	$A2	NACK
Length Invalid	$A3	NACK
Memory Access Error	$EE	ACK/NACK

7.14.5 Notes

The Read Checksum Option of the Read System Zone command is identical for 88SC and 88RF CryptoRF PICCs.

7.15 Verify Crypto Command [$c8]

The Verify Crypto command is used to activate the Authentication Communication Security mode and the Encryption Communication Security mode.

	Reader	PICC
Command >	CID, $8	
	Key Index	
	Q1	
	Q2	
	Q3	
	Q4	
	Q5	
	Q6	
	Q7	
	Q8	
	CH1	
	CH2	
	CH3	
	CH4	
	CH5	
	CH6	
	CH7	
	CH8	
	CRC1	
	CRC2	
Echo Command >		CID, $8
		ACK/NACK
		STATUS
		CRC1
		CRC2

7.15.1 Operation

The Verify Crypto command is used to perform mutual authentication between the PICC and the Host system. The Verify Crypto command is also used to activate the Encryption Communication Security mode.

Only PICCs in the Active State are permitted to answer this command.

7.15.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

Key Index: Selects the secret key to be used. The Authentication process uses one of the Secret Seeds G_i. Encryption Activation uses a Session Encryption Key S_i.

Table 7-37. Key Index Coding for the Verify Crypto Command

Key Index	Key
$00	Secret Seed G_0
$01	Secret Seed G_1
$02	Secret Seed G_2
$03	Secret Seed G_3
$10	Session Encryption Key S_0
$11	Session Encryption Key S_1
$12	Session Encryption Key S_2
$13	Session Encryption Key S_3
All Other Values Are Not Supported.	

Q: The Host random number.

CH: The Host challenge.

CRC: Communication error detection bytes.

7.15.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.15.4 Error Handling

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

Table 7-38. Status Codes returned in the Verify Crypto response

Error/Status Message	Status Code	Type
No errors	$00	ACK
Invalid Key Index	$99	NACK
Authentication or Encryption Activation Failure	$A9	NACK
Memory Access Error (Security Operation)	$F9	NACK
Memory Access Error	$EE	ACK/NACK

7.15.5 Notes

The Verify Crypto command is identical for 88SC and 88RF CryptoRF PICCs.

7.16 Send Checksum Command [$c9]

The Send Checksum command is used to authenticate data sent to the PICC in the Authentication Communication Security mode or the Encryption Communication Security mode.

	Reader	PICC
Command >	CID, $9 MAC1 MAC2 CRC1 CRC2	
Echo Command >		CID, $9 ACK/NACK STATUS CRC1 CRC2

7.16.1 Operation

When a Write User Zone command is sent in Authentication Communication mode or Encryption Communication mode the data received by the PICC is saved in a buffer until a cryptographic Checksum is received. The host uses the Send Checksum command to transmit the Checksum it has computed. If the checksum is valid the PICC writes the data; if the checksum is incorrect the data is discarded and the cryptographic engine is reset.

Only PICCs in the Active State are permitted to answer this command.

7.16.2 Command Field Description

CID: The Card ID assigned by the ATTRIB command.

MAC: The cryptographic checksum computed by the Host.

CRC: Communication error detection bytes.

7.16.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.16.4 Error Handling

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

Table 7-39. Status Codes Returned in the Send Checksum Response

Error/Status Message	Status Code	Type
Error/Status Message	Status Code	Type
No errors	$00	ACK
Checksum Failure	$C8	NACK
Checksum Failure	$C9	NACK
Memory Write Error - Data Mismatch	$ED	NACK
Memory Access Error	$EE	ACK/NACK

7.16.5 Notes

The Send Checksum command is identical for 88SC and 88RF CryptoRF PICCs.

7.17 DESELECT Command [$cA]

The DESELECT command places a PICC in the Halt State. This command is used at the end of a transaction.

	Reader	PICC
Command >	CID, $A CRC1 CRC2	
Echo Command >		CID, $A ACK STATUS CRC1 CRC2

7.17.1 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.

7.17.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

CRC: Communication error detection bytes.

7.17.3 Response Field Descriptions

CID: The PICC transmits its assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

7.17.4 Error Handling

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

Table 7-40. Status Codes Returned in the DESELECT Response

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

7.17.5 Notes

The HLTB command is identical for 88SC and 88RF CryptoRF PICCs.

7.18 IDLE Command [$cB]

The IDLE command resets the PICC and places it in the Idle State. This command is used at the end of a transaction.

	Reader	PICC
Command >	CID, $B CRC1 CRC2	
Echo Command >		CID, $B ACK STATUS CRC1 CRC2

7.18.1 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.

7.18.2 Command Field Descriptions

CID: The Card ID assigned by the ATTRIB command.

CRC: Communication error detection bytes.

7.18.3 Response Field Descriptions

CID: The PICC transmits its assigned card ID in the response.

ACK: Acknowledge, the command executed correctly.

STATUS: PICC status code.

CRC: Communication error detection bytes.

7.18.4 Error Handling

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

Table 7-41. Status Codes returned in the IDLE response

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

7.18.5 Notes

The HLTB command is identical for 88SC and 88RF CryptoRF PICCs.

7.19 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

7.19.1 Operation

To read or write data in User Zones that require a password for access the host must carry out a password validation operation. To write data to the Configuration Memory during personalization the host must carry out a transport 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.

If the Authentication Communication mode or the Encryption Communication mode is active, then the three PW bytes are encryptedNakedn Normal Communication mode the PW bytes are not encrypted.

7.19.2 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 7-42. Coding of the Password Index for 4-Kbit 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 7-43. Coding of the Password Index for 8-Kbit 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 Read 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.

7.19.3 Response Field Descriptions

CID: The PICC transmits its 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.

7.19.4 Error Handling

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

Table 7-44. Status Codes Returned in the Check Password Response

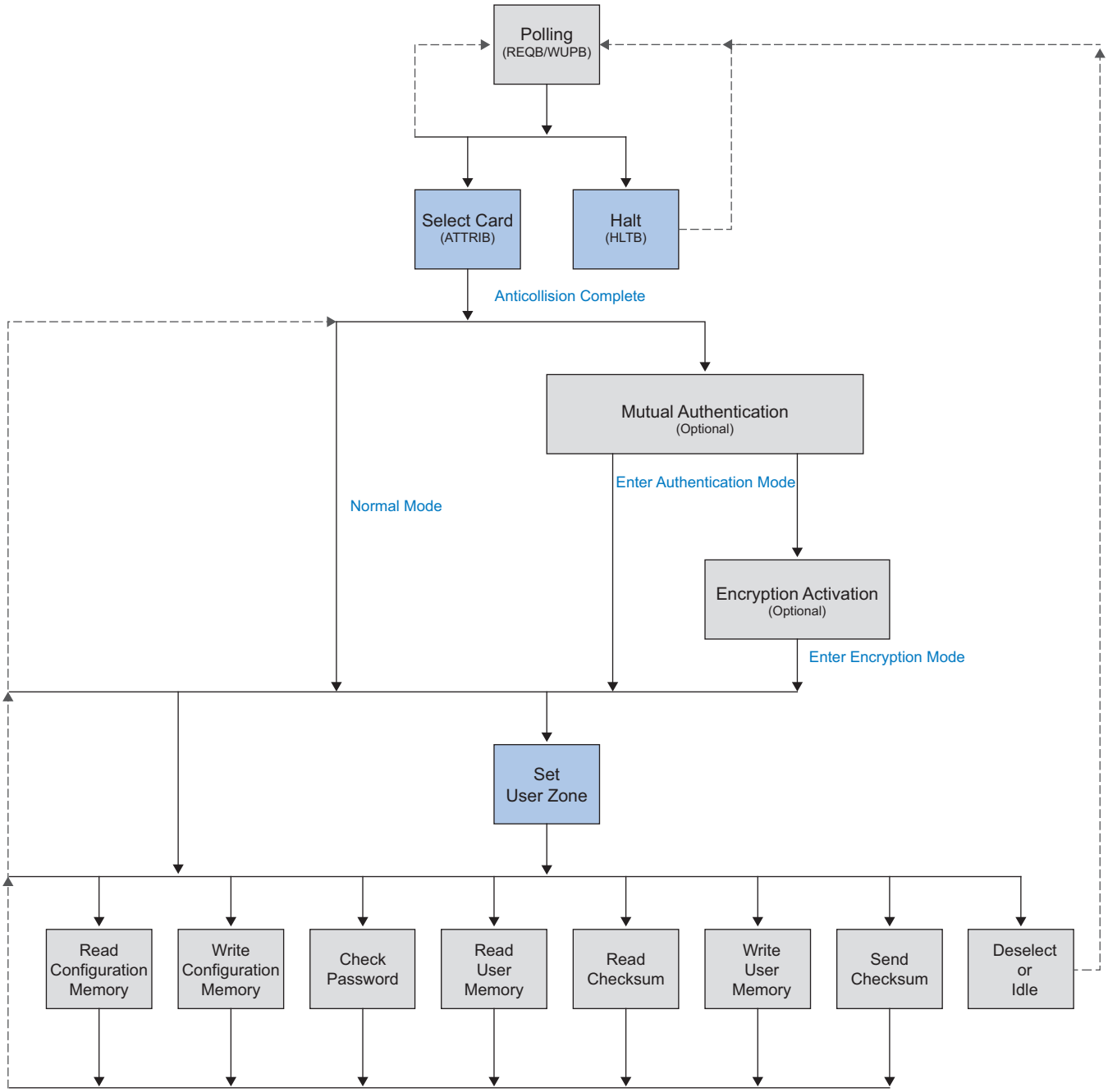
Error/Status Message	Status Code	Type
No errors	$00	ACK
Password Index Invalid	$A1	NACK
Check Password Failure	$D9	NACK
Memory Access Error (Security Operation)	$F9	NACK
Memory Access Error	$EE	ACK/NACK

7.19.5 Notes

The Check Password command is identical for 88SC and 88RF CryptoRF PICCs. Password indexes of $03 to $06, and $13 to $16 will be NACKed by 88RF PICCs.

8. Transaction Flow

Figure 8-1. 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: The Set User Zone command may be sent before or after the security operation.

9. Absolute Maximum Ratings*

Operating Temperature (Junction) . . .−25°C to +85°C

Storage Temperature (Ambient) . . . −65°C to + 150°C

HBM ESD (Antenna Pins only) . . . . . 2000V minimum

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

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.

10. Reliability

Table 10-1. Reliability

Parameter	Min	Typical	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.

11. Electrical Characteristics

Table 11-1. Electrical Characteristics[1]

Symbol	Parameter	Min	Nominal	Max	Units
C_T[2]	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

Notes: 1. Nominal values at 25°C. Values are based on characterization and are not tested.
2. Tuning Capacitance limits are specified at 25°C. C_T temperature coefficient is < 100ppm/°C.

11.1 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.

Appendix A Terms and Abbreviations

Abbreviation	Definition
88RF	Second generation CryptoRF devices. Catalog Number Series: AT88RFxxC
88SC	First generation CryptoRF devices. Catalog Number Series: AT88SCxxCRF
A	Unmodulated PCD field amplitude. Used in modulation index calculation.
AAC	Authentication Attempts Counter.
AAC_i	Authentication Attempts Counter with index i.
A/m	Amperes per Meter. Units of magnetic field strength.
AC	Alternating Current.
Access Control	Registers in the Configuration Memory that are reserved for security configuration.
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.
AK	Authentication Key. PR Register bits.
AM	Authentication Mode. AR Register mode control bit.
Anticollision	Registers in the Configuration Memory that are reserved for anticollision information.
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.
Auth	Authentication.
B	Modulated PCD field amplitude. Used in modulation index calculation.
C^A	Post Authentication Cryptogram calculated by Host for comparison with C_i^A
Card	A PICC with loop antenna in a plastic card or other RFID form factor.
Ch^A	Challenge from Host (for Mutual Authentication).
Ch^E	Challenge from Host (for Encryption Activation).
CH	Challenge calculated by CryptoRF for Comparison with Ch^A or Ch^E
C_i	Initial Cryptogram with Index i, stored in CryptoRF.
C_i^A	Cryptogram with Index i after Authentication, stored in CryptoRF.
CID	Card ID. The 4 bit code used to identify a PICC in the Active state.
C_i^E	Cryptogram with Index i after Encryption Activation, stored in CryptoRF.

Abbreviation	Definition
CMA	The third of four security fuses on 88SC PICCs.
CMC	Card Manufacturer Code. Register in Configuration Memory.
CRC	Cyclic Redundancy Check = 16 bit RF Communication Error Detection Code.
CRC_B	Cyclic Redundancy Check, Type B.
CRF	CryptoRF
CryptoMemory	A family of devices with CryptoRF security features and a TWI or ISO/IEC 7816 interface.
CryptoRF	CryptoRF. Catalog Number Series: AT88SCxxCRF and AT88RFxxC.
CryptoRF Reader	The Atmel ISO/IEC 14443 Type B reader IC. Catalog Number: AT88RF1354
Cryptography	Registers in the Configuration Memory that are reserved for security information.
C_T	Tuning Capacitance. The capacitance between antenna pins AC1 and AC2.
D	Variable for the Data bytes in a read or write Command.
D^E	Variable for the Encrypted Data Bytes in a read or write Command.
D(x)	Variable for a particular Data byte, byte x.
$D^E(x)$	Variable for a particular Encrypted Data byte, byte x.
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.
ENC	The second of four security fuses on 88RF PICCs.
EOF	End of Frame.
ER	Encryption Required. AR Register mode control bit.
ETA	Extended Trials Allowed. A DCR mode control bit on 88SC PICCs.
ETU	Elementary Time Unit = fc / 128 = 128 carrier cycles = 9.4395 uS nominal.
F1	A Function used by the Host for Authentication Key diversification.
F2	Any Function Performed Using the CryptoRF Cryptographic Engine.
FAB	The second of four security fuses on 88SC PICCs.
fc	Carrier Frequency = 13.56 MHz nominal.
Fo	Resonant Frequency.
FO	Frame Option.
Forbidden	Registers in the Configuration Memory that cannot be written or read.
fs	Subcarrier Frequency = fc/16 = 847.5 kHz nominal.
Fuse Byte	The contents returned when reading the Security Fuses.

Abbreviation	Definition
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.
G_i	Secret Seed with index i, stored in CryptoRF.
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.
HWR	Hardware Revision Register. [88RF PICCs]
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.
K	Secret Host Key. Diversified Keys are based on K.
KR	Key Register.
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.
M	Communication Security Mode. AR Register mode control bits.
MAC	Message Authentication Code. Checksum.
MDF	Modify Forbidden. AR 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.
µs	Microsecond
MSB	Most Significant Bit.
MTZ	Memory Test Zone. Address $0A and $0B in the Configuration Memory.

Abbreviation	Definition
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)
Nc	A 7 byte register that can be used for key diversification.
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.
Pgm	Program.
PGO	Program Only mode. AR Register mode control bit.
PICC	Proximity Integrated Circuit Card. The card/tag containing the IC and antenna.
PK	Primary Key. KR Register bits.
PM	Password Mode. AR Register mode control bit.
POK	Program Only Key. PR Register bits.
ppm	Parts Per Million.
PR	Password Register.
Protocol	Bytes communicating ISO protocol information.
PUPI	Pseudo Unique PICC Identifier. ID for anticollision.
PW	Password.
PW^E	Encrypted Password.
Q^A	Host Random Number generated by Host for Mutual Authentication.
Q^E	Host Random Number generated by Host for Encryption Activation.
R	Random number selected by PICC during anticollision.
RBmax	Receive Buffer size code. ATQB protocol byte returned by PICC.
RCS	Read Checksum. A DCR mode control bit on 88RF PICCs.
RF	Radio Frequency.
RFU	Reserved for Future Use. Any feature or bit reserved by ISO or by Atmel.
rms	Root Mean Square.
ROK	Read Only Key. KR Register bits.

Abbreviation	Definition
ROM	Read-Only Memory.
RW	REQB/WUPB command selection code.
S	Slot Number. A code sent to the PICC with Slot MARKER command.
S^A	Session Key calculated by CMC during Mutual Authentication.
S_i^A	Session Key calculated by CryptoRF during Mutual Authentication.
SEC	The first of four security fuses.
SKY	The third of four security fuses on 88RF PICCs.
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 one of several non-credit card form factors.
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.
UAT	Unlimited Authentication Trials. A DCR mode control bit.
UCR	Unlimited Checksum Read. A DCR mode control bit on 88SC PICCs.
UDSN	Unique Die Serial Number. Read-only register in the Configuration Memory
UZ	User Zone.
WCS	Write Checksum Timeout. A DCR mode control bit on 88RF PICCs.
WG8	ISO/IEC Working Group eight. Develops standards for contactless smartcards.
WLM	Write Lock Mode. AR Register mode control bit on 88SC PICCs.
WUPB	Wake Up command, Type B.
z	Variable for the Index of a Password Set or Key Set.

Appendix 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 106kbps 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 14443-1:2008	*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 a 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 2056 available at www.atmel.com.

CryptoRF Ordering Codes: *CryptoRF and Secure RF Standard Product Offerings*. Document 5047 available at www.atmel.com.

Appendix 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 Appendix H for additional 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
AT88RF04C	4K	512K	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: 1. 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.

Table C-2. Atmel AT88RF04C 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								

Table C-3. Atmel 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								

Table C-4. Atmel 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								

Table C-4. Atmel AT88SC1616CRF Memory Map for 16-Kbit User Memory (Continued)

Zone		$0	$1	$2	$3	$4	$5	$6	$7
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								
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								

Table C-5. Atmel 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								
User 11	$00								
	—	256 bytes							
	$F8								
User 12	$00								
	—	256 bytes							
	$F8								

Table C-5. Atmel AT88SC3216CRF Memory Map for 32-Kbit User Memory (Continued)

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 13	$00								
	—	256 bytes							
	$F8								
User 14	$00								
	—	256 bytes							
	$F8								
User 15	$00								
	—	256 bytes							
	$F8								

Table C-6. Atmel 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								

Table C-6. Atmel AT88SC6416CRF Memory Map for 64-Kbit User Memory (Continued)

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 8	$000								
	—	512 bytes							
	$1F8								
User 9	$000								
	—	512 bytes							
	$1F8								
User 10	$000								
	—	512 bytes							
	$1F8								
User 11	$000								
	—	512 bytes							
	$1F8								
User 12	$000								
	—	512 bytes							
	$1F8								
User 13	$000								
	—	512 bytes							
	$1F8								
User 14	$000								
	—	512 bytes							
	$1F8								
User 15	$000								
	—	512 bytes							
	$1F8								

Appendix 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	
	Sets	Set Number	Sets	Free for Customer Use	PW Index	Password
AT88RF04C	4	0,1,2,7	4	25 bytes	$07	$30 1D D2
AT88SC0808CRF	8	0,1,2,3,4,5,6,7	4	27 bytes	$07	$40 7F AB
AT88SC1616CRF	8	0,1,2,3,4,5,6,7	4	27 bytes	$07	$50 44 72
AT88SC3216CRF	8	0,1,2,3,4,5,6,7	4	27 bytes	$07	$60 78 AF
AT88SC6416CRF	8	0,1,2,3,4,5,6,7	4	27 bytes	$07	$70 BA 2E

Access rights to the Configuration Memory are fixed in logic and are controlled by the security fuses. See Appendix G 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 on 88SC PICCs and 25 bytes of OTP memory are available on 88RF PICCs, all other registers have assigned functionality. The OTP memory bytes available for customer use are described in Appendix E

Table D-2. Configuration Memory Map for Atmel AT88RF04C

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	MTZ		CMC		HWR		
$10	Unique Die Serial Number								Read only
$18	DCR	Identification Number Nc							Access Control
$20	AR0	KR0	AR1	KR1	AR2	KR2	AR3	KR3	
$28	Reserved								
$30									
$38									
$40	Issuer Code								
$48									
$50	AAC_0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC_1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC_2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC_3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	Reserved								
$D0									
$D8									
$E0									
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

Table D-3. Configuration Memory Map for Atmel AT88SC0808CRF

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	MTZ		CMC				
$10	Unique Die Serial Number								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	AAC_0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC_1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC_2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC_3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read 3			
$D0	PAC	Write 4			PAC	Read 4			
$D8	PAC	Write 5			PAC	Read 5			
$E0	PAC	Write 6			PAC	Read 6			
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

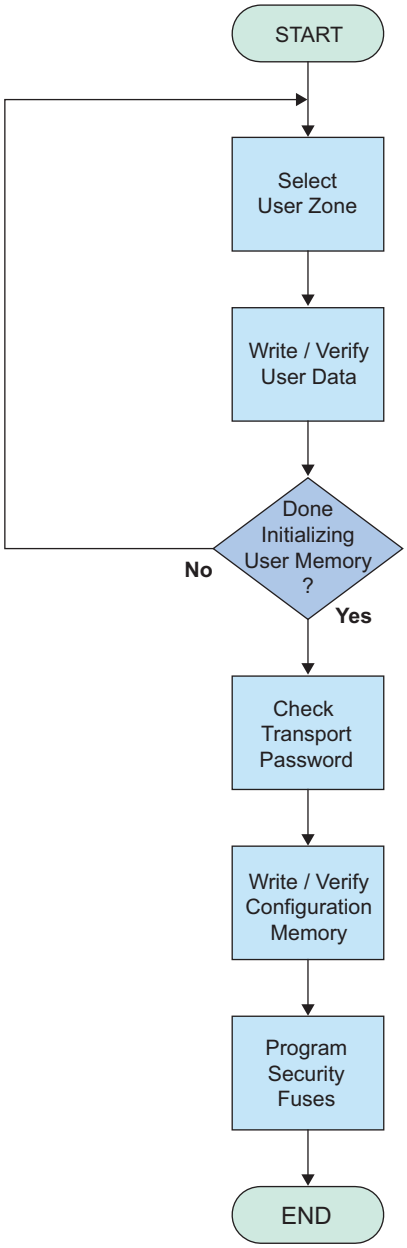
Table D-4. Configuration Memory Map for Atmel AT88SC1616CRF, AT88SC3216CRF, and AT88SC6416CRF

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	MTZ		CMC				
$10	Unique Die Serial Number								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	AAC_0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC_1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC_2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC_3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read 3			
$D0	PAC	Write 4			PAC	Read 4			
$D8	PAC	Write 5			PAC	Read 5			
$E0	PAC	Write 6			PAC	Read 6			
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

Appendix E Device Personalization

CryptoRF is delivered with the user memory filled with $FF data and with the 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 the 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. Table H-3 shows the polling response registers in blue, OTP memory in green, and access control registers in gray. The Unique Die Serial Number register is factory programmed and cannot be changed.

There are 27 bytes of OTP memory available for customer use in 88SC PICCs, and 25 bytes in 88RF PICCs; these registers are shown in green in Table H-3 and Table H-4. See Appendix M for detailed information on configuration of the polling response registers. See Appendix H for detailed information on configuration of the access control registers.

Figure E-2. System Zone Map for 88SC PICCs 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">CMC</td></tr>
<tr><td>$10</td><td colspan="8">Unique Die Serial Number</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>

Figure E-3. System Zone Map for 88RF PICCs 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="2">CMC</td><td colspan="2">HWR</td></tr>
<tr><td>$10</td><td colspan="8">Unique Die Serial Number</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 two 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 16-bit or 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.

Hardware Revision (HWR) [88RF]

This 16-bit register is defined by Atmel. This code identifies the hardware type and design revision. This code cannot be modified. The HWR code for 88RF PICCs is $C2XX where XX is the design revision code.

Unique Die Serial Number (UDSN)

This 64-bit register is defined by Atmel. This code contains a unique serial number for each die and manufacturing traceability data. This code cannot be modified. [This register was previously named “Lot History Code”.]

Atmel reserves the right to modify the format of the contents of the UDSN register without notice; however, the UDSN register value is guaranteed to be unique for each die.

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
AT88RF04C	$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 or ENC fuse.
2. Send Write System Zone command with:
   PARAM = $01, ADDR = $04, L = $00, DATA = $00 to program the CMA or SKY 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.

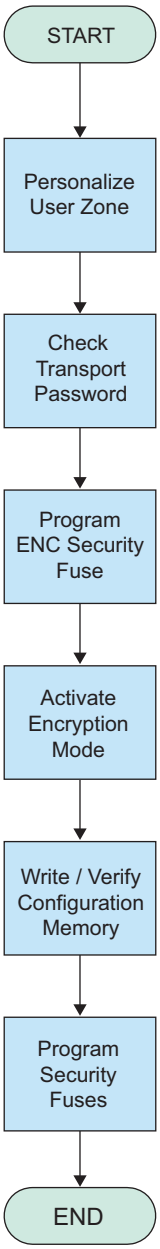
E.5 Secure Personalization

The 88RF PICCs support an optional encrypted personalization mode for programming the device secrets. The Secure Personalization option is described in Appendix F This option is not available on 88SC PICCs.

Appendix F Secure Personalization [88RF]

This appendix describes the optional Secure Personalization mode for 88RF PICCs. This mode allows the device secrets to be written with data encryption, so that eavesdropping on the personalization process cannot compromise the device secrets.

Figure F-1. Secure Personalization Process Flowchart



F.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 automatically verified by the Automatic Data Write function as each Write User Zone command is processed. The data can also be verified with Read User Zone commands. Each User Zone is programmed in this manner.

F.2 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 88RF device is shown in Table F-1. The Transport Password is the same for every device with the same base part number; it is never changed by Atmel.

Table F-1. 88RF PICC Transport Passwords

CryptoRF Part Number	Transport Password	
	PW Index	Password
AT88RF04C	$07	$30 1D D2

F.3 Security Fuse Programming

The optional Secure Personalization mode is enabled and disabled by programming the security fuses. By default the Secure Personalization mode is disabled. Programming the ENC fuse enables Secure Personalization mode.

Three security fuses are programmed during 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 ENC (Encryption) fuse. The Secure Personalization mode is enabled by programming the ENC fuse.
2. Send Write System Zone command with:
   PARAM = $01, ADDR = $04, L = $00, DATA = $00 to program the SKY (Secret Key) fuse. The secrets are locked and the Secure Personalization mode is disabled by programming the SKY fuse.
3. Send Write System Zone command with:
   PARAM = $01, ADDR = $00, L = $00, DATA = $00 to program the PER (Personalization) fuse. The Transport Password is disabled by programming 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.

F.4 Secure Personalization Mode Data Encryption

When the optional Secure Personalization mode is enabled by programming the ENC fuse to 0b, then certain registers in the configuration memory require communication encryption for read or write access. This is shown in Table F-2 below using color codes. The contents of registers with green shading are never encrypted when reading or writing, regardless of the communication security mode of the PICC. Access to registers with pink shading is forbidden; no read or write access is allowed.

The registers shaded in blue contain device “secrets”, they cannot be written or read unless the Encryption Communication Security mode has been activated (with any key set). The contents of these “secrets” registers is encrypted when reading or writing. Use of the Write System Zone with Integrated MAC command is mandatory when writing the “secrets” registers (see Section 7.10).

Table F-2. Configuration Memory Map Showing Data Encryption Requirements for Fuse State ENC = 0b, SKY = 1b.

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	PUPI				APP				Anticollision
$08	RBmax	AFI	MTZ		CMC		HWR		
$10	Unique Die Serial Number								Read only
$18	DCR	Identification Number Nc							Access Control
$20	AR0	KR0	AR1	KR1	AR2	KR2	AR3	KR3	
$28	Reserved								
$30									
$38									
$40	Issuer Code								
$48									
$50	AAC_0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC_1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC_2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC_3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								
$B0	PAC	Write 0			PAC	Read 0			Password
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	Reserved								
$D0									
$D8									
$E0									
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								Forbidden
$F8									

Programming the SKY fuse locks the Secret Seeds and Session Encryption Key registers so that the contents cannot be read or changed. Once locked, these registers cannot be unlocked. The SKY fuse also disables the Secure Personalization mode and disables the Write System Zone with Integrated MAC command.

The Configuration Memory Access requirements for all four of the Security Fuse states is described in Appendix G

Note: It is not necessary to initialize the Session Encryption Key registers since any data contained in these registers will be overwritten by the first Authentication Activation attempt.

Appendix G 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, Keys, and other configuration data during the personalization process so that they cannot be changed after a card is issued.

G.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 four to seven of this byte are not used as security fuses and are reserved by Atmel.

Figure G-1. Definition of the DATA Byte received when reading the Fuse Byte of 88SC PICCs.

F7	F6	F5	F4	F3	F2	F1	F0	
RFU	*RFU*	*RFU*	*RFU*	SEC	PER	CMA	FAB	
X	X	X	X	0	1	1	1	Default Value

Figure G-2. Definition of the DATA Byte received when reading the Fuse Byte of 88RF PICCs.

F7	F6	F5	F4	F3	F2	F1	F0	
RFU	*RFU*	*RFU*	*RFU*	SEC	ENC	SKY	PER	
X	X	X	X	0	1	1	1	Default Value

G.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:

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

G.3 Configuration Memory Access Control

Table G-1 shows the Configuration Memory access conditions for each of the 88SC PICC security fuse settings. Table G-2 shows the Configuration Memory access conditions for each of the 88RF PICC 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 states.

The default state of the fuses when CryptoRF leaves the factory is SEC = 0b and the remaining three fuses set to 1b. The left fuse column in Table G-1 and Table G-2 show the access conditions for this default fuse state.

Table G-1. Configuration Memory Access control by Security Fuse State for 88SC PICCs.

Registers	Operation	Fuse State			
		SEC = 0b FAB = 1b CMA = 1b PER = 1b	SEC = 0b FAB = 0b CMA = 1b PER = 1b	SEC = 0b FAB = 0b CMA = 0b PER = 1b	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 Attempt 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 G-1 and Table G-2 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. Blue fields indicate that Encryption Activation is required for access.

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.

Table G-2. Configuration Memory Access control by Security Fuse State for 88RF PICCs.

Registers	Operation	Fuse State			
		SEC = 0b ENC = 1b SKY = 1b PER = 1b	SEC = 0b ENC = 0b SKY = 1b PER = 1b	SEC = 0b ENC = 0b SKY = 0b PER = 1b	SEC = 0b ENC = 0b SKY = 0b PER = 0b
Anticollision (Except MTZ, HWR)	Read	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Transport PW	Forbidden
Memory Test Zone (MTZ)	Read	Open	Open	Open	Open
	Write				
Hardware Revision (HWR)	Read	Open	Open	Open	Open
	Write	Forbidden	Forbidden	Forbidden	Forbidden
Read Only (Unique Die Serial Number)	Read	Open	Open	Open	Open
	Write	Forbidden	Forbidden	Forbidden	Forbidden
Access Control (Except Nc, DCR)	Read	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Transport PW	Forbidden
Nc and DCR	Read	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Forbidden	Forbidden
Cryptography (Except Encryption Keys S)	Read	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Forbidden	Forbidden
Encryption Keys (S)	Read	Transport PW	Transport PW + Encryption	Forbidden	Forbidden
	Write				
Secret	Read	Transport PW	Transport PW + Encryption	Forbidden	Forbidden
	Write				
Passwords	Read	Transport PW	Transport PW + Encryption	Transport PW	Write PW
	Write				
Password Attempt Counters (PAC)	Read	Open	Open	Open	Open
	Write	Transport PW	Transport PW	Transport PW	Write PW
Forbidden	Read	Forbidden	Forbidden	Forbidden	Forbidden
	Write				

Appendix H 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 Registers (AR) 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 appendix.

H.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 (PR) or Key Register (KR) 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 for 88SC PICCs, 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.

H.1.1 Access Registers (AR) [88SC]

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 H-1. Definition of the User Zone Access Registers for 88SC PICCs.

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

The Access Register definition for 88SC PICCs is shown in Figure H-1. 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 H-1. 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 H-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	

AM: Authentication Mode selection bits.

The three Communication Security Mode control bits: AM0, AM1, and ER control the communication security requirements for the User Zone as shown in Table H-2. By default authentication and encryption communication security are disabled. See Appendix J for information on the Authentication Communication Security modes.

ER: Encryption Mode selection bit.

The three Communication Security Mode control bits: AM0, AM1, and ER control the communication security requirements for the User Zone as shown in Table H-2. By default authentication and encryption communication security are disabled. See Appendix K for information on Encryption Communication Security.

Table H-2. Communication Security Mode Options for 88SC PICCs.

AM1	AM0	ER	Communication Security Mode	Auth. Key (AK)	Pgm-Only Key (POK)
0	0	0	Reserved For Future Use (Not Supported)	N/A	N/A
0	0	1	Dual Access Authentication Mode	Read/Write Access	Read / Program Access
0	1	0	Reserved For Future Use (Not Supported)	N/A	N/A
0	1	1	Authentication for Read / Write	Read/Write Access	N/A
1	0	0	Reserved For Future Use (Not Supported)	N/A	N/A
1	0	1	Authentication for Write	Read/Write Access	N/A
1	1	0	Encryption for Read / Write	Read/Write Access	N/A
1	1	1	No Authentication or Encryption Required	N/A	N/A

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 eight byte pages with the first byte of each page controlling write access to all eight bytes. Figure H-2 shows an example of WLM on two contiguous eight byte pages.

Figure H-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 eight 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 seven controls byte seven, bit six controls byte six, etc.

Note: 1. 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: When PGO is enabled, Write User Zone commands are restricted to a length of one byte.

H.2 Access Registers (AR) [88RF]

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 H-3. Definition of the Access Register for User Zone 1 of 88RF PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
PM1	PM0	M2	M1	M0	RFU	MDF	PGO	
1	1	1	1	1	1	1	1	Default Value

Figure H-4. Definition of the Access Register for User Zones 0, 2, and 3 of 88RF PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
PM1	PM0	M2	M1	M0	RFU	MDF	RFU	
1	1	1	1	1	1	1	1	Default Value

The Access Register definition is shown in Figure H-3 and Figure H-4. Bit two is reserved for future use. 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 H-3. 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 Key Register.

Table H-3. 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	

M: Communication Security Mode control.

The Access Register M bits determine the Communication Security mode requirements for the User Zone. By default, M = 111b and no Authentication or Encryption Activation is required to access the user memory.

Table H-4. Communication Security Mode Options for 88RF PICCs

M2	M1	M0	Communication Security Mode	Primary Key (PK)	Read-Only Key (ROK)
0	0	0	Reserved For Future Use (Not Supported)	N/A	N/A
0	0	1	Reserved For Future Use (Not Supported)	N/A	N/A
0	1	0	Authentication for Read/Encryption for Write	Read / Write Access	Read Access
0	1	1	Authentication for Read/Write	Read / Write Access	Read Access
1	0	0	Encryption for Write	Read / Write Access	N/A
1	0	1	Authentication for Write	Read / Write Access	N/A
1	1	0	Encryption for Read/Write	Read / Write Access	Read Access
1	1	1	No Authentication or Encryption Required	N/A	N/A

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: PGO is only available in User Zone 1. If PGO is enabled, then the Write User Zone data verification function is disabled when writing to User Zone 1 of 88RF PICCs. The PGO option is not available in User Zones 0, 2, and 3 of 88RF PICCs.

H.2.1 Password Registers (PR) [88SC]

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

Figure H-5. Definition of the User Zone Password Registers on 88SC PICCs.

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

The Password Register bit definitions are shown in Figure H-5. Changes to the PR registers are effective immediately.

AK: Authentication Key Set selection bits.

The Authentication Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register bits determine the Communication Security mode. Any number of PR registers can point to the same key set, allowing multiple User Zones to use the same key set.

Table H-5. Coding of the Authentication Key Set Select Bits for CryptoRF Communication Security

AK1	AK0	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

POK: Program-Only Key Set selection bits.

The Program-Only Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register bits determine the Communication Security mode. The POK bits are only used if Dual Access Authentication mode has been selected. Any number of PR registers can point to the same key set, allowing multiple User Zones to use the same key set.

Table H-6. Coding of the Program-Only Key Set Select Bits for CryptoRF Communication Security

POK1	POK0	Authentication Key
0	0	Secret Seed G_0
0	1	Secret Seed G_1
1	0	Secret Seed G_2
1	1	Secret Seed G_3

PW: Password Set selection bits.

The Password Set selection bits control the password set assigned to a User Zone. Table H-7 shows 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 H-7. Coding of the Password Set Select Bits for the 8-Kbit 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

H.2.2 Key Registers (KR) [88RF]

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

Figure H-6. Definition of the User Zone Key Registers for 88RF PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
PK1	PK2	ROK1	ROK2	RFU	PW2	PW1	PW0	
1	1	1	1	1	1	1	1	Default Value

The Key Register bit definitions are shown in Figure H-6. Changes to the KR registers are effective immediately.

PK: Primary Key Set selection bits.

The Primary Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register M bits determine the Communication Security mode associated with the PK bits.

Table H-8. Coding of the Primary Key Set Select Bits for CryptoRF communication Security on 88RF PICCs

PK1	PK2	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

ROK: Read-Only Key Set selection bits.

The Read-Only Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register M bits determine the Communication Security mode associated with the ROK bits.

Table H-9. Coding of the Read-Only Key Set Select Bits for CryptoRF communication Security on 88RF PICCs

ROK1	ROK2	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

PW: Password Set selection bits.

The Password Set selection bits control the password set assigned to a User Zone. Table H-10 shows the coding of these register bits. Any number of KR registers can point to the same password set, allowing multiple User Zones to use the same password set.

Table H-10. Coding of the Password Set Select Bits on 88RF PICCs

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 Support*ed.			

H.3 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).

H.3.1 Device Configuration Register (DCR)

There is one Device Configuration Register in each PICC. The default state of this register is $FF for 88SC PICCs and $7C for 88RF PICCs.

Figure H-7. Definition of the Device Configuration Register for 88SC PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
SME	UCR	UAT	ETA	EGTL	RFU	RFU	RFU	
1	1	1	1	1	1	1	1	Default Value

Figure H-8. Definition of the Device Configuration Register for 88RF PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
SME	RFU	UAT	RFU	EGTL	RFU	WCS	RCS	
1	1	1	1	1	1	1	1	Default Value

The DCR register definition is shown in Figure H-7 and Figure H-8. Bits zero, one, and two are reserved for future use. Changes to the DCR are effective at the next Power-On or anticollision sequence.

SME: Supervisor Mode Enable control.

By default, the Supervisor Mode is disabled on 88SC PICCs and enabled on 88RF PICCs. 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.

UCR: Unlimited Checksum Read control. [88SC]

By default, the UCR is disabled. If UCR = 0b, then Unlimited Checksum Reads are enabled. This function is intended for development use only, since it allows systematic attacks on the security. This function does not affect the Password Attempts Counters (PACs).

UAT: Unlimited Authentication Trials control.

By default, the UAT is disabled. If UAT = 0b, then the Authentication Attempts Counters (AACs) are disabled for all key sets. This function is intended for development use only, since it allows systematic attacks on the security. This function does not affect the Password Attempts Counters (PACs).

ETA: Extended Trials Allowed control. [88SC]

By default, the Extended Trials Allowed option is disabled. If this option is enabled by setting ETA = 0b, then the maximum number of authentication and password trials is increased to permit a maximum of eight attempts before a password or key is locked. If ETA is disabled, then only four 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 Appendix O for information about EGT.

WCS: Write Checksum Timeout control. [88RF]

By default, the WCS is enabled. In authentication and encryption communication security modes the correct checksum must be provided within 77ms, or the write operation is aborted. Setting WCS = 1b disables the timeout function.

RCS: Read Checksum control. [88RF]

By default, the RCS is enabled which allows one Read Checksum operation without resetting the cryptographic engine.

Appendix I 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.

I.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 I-1. CryptoRF Communication Security Options

Communication Mode	User Data	System Data	Passwords
Normal	Clear	Clear	Clear
Authentication	Clear	Clear	Encryption
Encryption	Encryption	Clear[(1)]	Encryption

Note: 1. 88RF PICCs support an encryption option for programming secrets. See Appendix F.

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

I.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 I-2. CryptoRF Family Password Characteristics and Transport Passwords

CryptoRF Part Number	Password Sets		Transport Password	
	Sets	Set Number	PW Index	Password
AT88RF04C	4	0,1,2,7	$07	$30 1D D2
AT88SC0808CRF	8	0,1,2,3,4,5,6,7	$07	$40 7F AB
AT88SC1616CRF	8	0,1,2,3,4,5,6,7	$07	$50 44 72
AT88SC3216CRF	8	0,1,2,3,4,5,6,7	$07	$60 78 AF
AT88SC6416CRF	8	0,1,2,3,4,5,6,7	$07	$70 BA 2E

I.3 The Password and PAC Registers

Each password set, along with its associated Password Attempt Counters, is stored in an eight byte segment in the Password section of the Configuration Memory. Figure I-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 I-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	PW3

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 I-1.

Table I-3. Password Attempt Counter Coding for the Default DCR Configuration of 88SC PICCs

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 I-4. Password Attempt Counter Coding for the Extended Trials Allowed DCR Configuration of 88SC PICCs

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.	

Table I-5. Password Attempt Counter Coding for 88RF PICCs

PAC Register	Description
$55	No Failed Attempts
$56	1 Failed Attempt
$59	2 Failed Attempts
$5A	3 Failed Attempts
$65	4 Failed Attempts
$66	5 Failed Attempts
$69	6 Failed Attempts
$6A	7 Failed Attempts
$95	8 Failed Attempts
$96	9 Failed Attempts
$99	10 Failed Attempts
$9A	11 Failed Attempts
$A5	12 Failed Attempts
$A6	13 Failed Attempts
$A9	14 Failed Attempts
$AA	15 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 I-3, Table I-4, and Table I-5 show coding of the PAC register. On 88SC PICCs, the DCR register bit ETA selects the number of password attempt that are permitted; the default configuration allows four attempts, ETA = 0b allows eight attempts. On 88RF PICCs the maximum number of attempts is fifteen. If the PAC reaches the maximum count, then the corresponding password is locked and all subsequent Check Password commands will fail.

I.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 Register for the zone. Configuration of the registers is described in Appendix H.

Table I-6. 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 I-6 shows the available password security options. The default setting of PM=11b 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.

I.5 Password Verification

A password is sent for verification using the Check Password command as shown in Figure I-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 show no failed attempts, and return an ACK in the response.

The internal password security status register maintains its state 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: 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 I-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 “Check Password Command [$cC]” on page 64 for a description of the Status codes.

Table I-7. 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 PICC information.
Password Attempts Count				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 for 88SC PICCs. The upper nibble of the NACK byte is the number of failed attempts (one to eight failures), while the lower nibble is the NACK code $1.

For 88RF PICCs this special NACK will contain one of the following values: $11, $21, $31, $41, $51, $61, $71, $81, $91, $A1, $B1, $C1, $D1, $E1, $F1. The upper nibble of the NACK byte is the number of failed attempts (1 to 15 failures), while the lower nibble is the NACK code $1.

If failure of the Check Password command does not results in the Password Attempt Counter being incremented, then the NACK byte will contain $01.

I.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 in the DCR, then the Supervisor Password can be used to enable write access to the passwords unless the Supervisor Password is also locked.

I.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.

Appendix J Using Authentication Communication 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 Authentication Communication Security on a User Zone restricts access to the data to users with knowledge of the Authentication key.

J.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 Communication Security mode encrypts only passwords. Encryption Communication Security mode encrypts both user data and passwords. The default communication mode is Normal mode.

Table J-1. CryptoRF Communication Security Options

Communication Mode	User Data	System Data	Passwords
Normal	Clear	Clear	Clear
Authentication	Clear	Clear	Encryption
Encryption	Encryption	Clear[(1)]	Encryption

Note: 1. 88RF PICCs support an encryption option for programming secrets. See Appendix F.

Authentication Communication Security is activated by performing Mutual Authentication between the Host system and the PICC using the Verify Crypto command. Once activated, the PICC will remain in Authentication mode until a security error occurs, a new Verify Crypto command is received, RF power is removed, or a DESELECT command or IDLE command is received.

J.2 Authentication Security Options [88SC]

Authentication Communication Security for a User Zone is enabled by programming the Access Register (AR) and Password Register (PR) for the zone. The Communication Security Mode (M) bits [AM1, AM0, ER] of the Access Register determine the Communication Security requirements for the User Zone. The Password Register determines which Key Set(s) are used to access the User Zone. Configuration of the AR and PR registers is described in Appendix H

Table J-2. Selecting Authentication using the Communication Security Mode bits of the Access Register.

AM1	AM0	ER	Communication Security Mode	Auth. Key (AK)	Pgm-Only Key (POK)
0	0	1	Dual Access Authentication Mode	Read/Write Access	Read/Program Access
0	1	1	Authentication for Read/Write	Read/Write Access	N/A
1	0	1	Authentication for Write	Read/Write Access	N/A
1	1	1	No Authentication or Encryption Required	N/A	N/A

Table J-2 shows the three 88SC PICC Authentication Communication Security options, plus the default setting. By default M = 111b and no Authentication or Encryption Activation is required to access the user memory.

J.2.1 M = 001b Security — Dual Access Authentication Mode

When M = 001b Authentication is required for Read or Write access to the User Zone. If Authentication is performed with the key identified in the POK bits of the Password Register, then Read and Program-Only access is granted to the User Zone. In this state data may be changed from 1b to 0b, but never from 0b to 1b.

If Authentication is performed with the key identified in the AK bits of the Password Register, then full Read/Write access is granted to the User Zone. A checksum is required for write operations.

J.2.2 M = 011b Security – Authentication for Read/Write

When M = 011b Authentication is required for Read or Write access to the User Zone. If Authentication is performed with the key identified in the AK bits of the Password Register, then Read/Write access is granted to the User Zone. A checksum is required for write operations.

J.2.3 M = 101b Security – Authentication for Write

When M = 101b Authentication is required for Write access to the User Zone. If Authentication is performed with the key identified in the AK bits of the Password Register, then Read/Write access is granted to the User Zone. Read-Only access does not require Authentication or Encryption Activation. A checksum is required for write operations.

J.3 Authentication Security Options [88RF]

Authentication Communication Security for a User Zone is enabled by programming the Access Register (AR) and Key Register (KR) for the zone. The Communication Security Mode (M) bits of the Access Register determine the Communication Security requirements for the User Zone. The Key Register determines which Key Set(s) are used to access the User Zone. Configuration of the AR and KR registers is described in Appendix H.

Table J-3. Selecting Authentication Using the Communication Security Mode Bits of the Access Register

M2	M1	M0	Communication Security Mode	Primary Key (PK)	Read-Only Key (ROK)
0	1	0	Authentication for Read/Encryption for Write	Read/Write Access	Read Access
0	1	1	Authentication for Read/Write	Read/Write Access	Read Access
1	0	1	Authentication for Write	Read/Write Access	N/A
1	1	1	No Authentication or Encryption Required	N/A	N/A

Table J-3 shows the three 88RF PICC Authentication Security options, plus the default setting. By default M = 111b and no Authentication or Encryption Activation is required to access the user memory.

J.3.1 M = 010b Security - Authentication for Read / Encryption for Write

When M = 010b Authentication is required for Read access to the User Zone. Encryption Activation is required for Write Access to the User Zone. If Authentication is performed with the key identified in the ROK bits of the Key Register, then Read-Only access is granted to the User Zone. If Encryption Activation is performed with the key identified in the PK bits of the Key Register, then Read/Write access is granted to the User Zone. A checksum is required for write operations.

The M = 010b mode is a new feature in 88RF PICCs. This mode is not available in 88SC devices.

J.3.2 M = 011b Security - Authentication for Read / Write

When M = 011b Authentication is required for Read or Write access to the User Zone. If Authentication is performed with the key identified in the PK bits of the Key Register, then Read/Write access is granted to the User Zone. If Authentication is performed with the key identified in the ROK bits of the Key Register, then Read-Only access is granted to the User Zone. A checksum is required for write operations.

If the PK and ROK bits of the Key Register select the same Key Set, then the Read-Only function is effectively disabled. Authenticating 88RF PICCs with the PK key results in behavior identical to 88SC devices. The Read-Only function is not supported by 88SC devices.

J.3.3 M = 101b Security - Authentication for Write

When M = 101b Authentication is required for Write access to the User Zone. If Authentication is performed with the key identified in the PK bits of the Key Register, then Read/Write access is granted to the User Zone. Read-Only access does not require Authentication or Encryption Activation. A checksum is required for write operations.

88RF PICC behavior is identical to 88SC devices when M = 101b.

J.4 The Password Register [88SC]

The Password Registers are used to select the Key Sets for Authentication or Encryption Communication Security. Any Key Set can be used with any User Zone by programming the Key Register for the User Zone with the appropriate AK and POK values. One Key Set can be used with any number of User Zones.

Figure J-1. Definition of the User Zone Password Registers on 88SC PICCs

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

The Authentication Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register bits determine the Communication Security mode associated with the AK bits.

Table J-4. Coding of the Authentication Key Set Select Bits for CryptoRF Communication Security

AK1	AK0	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

The Program-Only Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register bits determine the Communication Security mode associated with the POK bits. The POK bits are only used in Dual Access Authentication mode.

Table J-5. Coding of the Program-Only Key Set Select Bits for CryptoRF Communication Security

POK1	POK0	Authentication Key
0	0	Secret Seed G_0
0	1	Secret Seed G_1
1	0	Secret Seed G_2
1	1	Secret Seed G_3

J.5 The Key Register [88RF]

The Key Registers are used to select the Key Sets for Authentication or Encryption Communication Security. Any Key Set can be used with any User Zone by programming the Key Register for the User Zone with the appropriate PK and ROK values. One Key Set can be used with any number of User Zones.

Figure J-2. Definition of the Key Registers on 88RF PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
PK1	PK2	ROK1	ROK2	RFU	PW2	PW1	PW0	
1	1	1	1	1	1	1	1	Default Value

The Primary Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register M bits determine the Communication Security mode associated with the PK bits.

Table J-6. Coding of the Primary Key Set Select Bits

PK1	PK2	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

The Read-Only Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register M bits determine the Communication Security mode associated with the ROK bits. For some Communication Security modes the ROK register bits are not used.

Table J-7. Coding of the Read-Only Key Set Select Bits

ROK1	ROK2	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

J.6 Key Sets

CryptoRF has four Key Sets. Each Key Set is associated with four registers in the Configuration Memory. The Authentication Key is stored in the Secret Seed G_i register. The Authentication Attempt Counter for Secret Seed G_i is stored in the AAC_i register. The Cryptogram C_i register is used during Authentication Activation procedure to store the response to the Host challenge. The Session Key S_i register is used to store the Encryption Activation key.

Figure J-3. Partial Configuration Memory Map Showing the Key Set Registers

	$0	$1	$2	$3	$4	$5	$6	$7	
$50	AAC_0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC_1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC_2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC_3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								

Figure J-3 shows the portion of the Configuration Memory that contains the Key Set registers. The registers shaded in green can always be read, but cannot be written after personalization. The registers shaded in blue cannot be written or read after personalization.

Note: All of the Security Fuses must be programmed during personalization for the device secrets to be secure.

Key Set i uses registers AAC_i, C_i, G_i, and S_i. If AAC_i is locked, the Key Set i is permanently disabled and any User Zone requiring Key Set i for Authentication or Encryption Activation will no longer be accessible.

J.6.1 Changing Keys

The Secret Seeds cannot be modified after the Security Fuses are programmed during personalization. The AAC registers cannot be re-written after the Security Fuses are programmed either. This is true even if the SME option in the DCR register is enabled.

J.7 AAC Registers

The Authentication Attempt Counters contain a value which indicates how many unsuccessful Authentication attempts have been made using the Key Index of the corresponding Secret Seed. Table J-8, Table J-9 and Table J-10 shows coding of the AAC register. If the AAC reaches the maximum count of four or eight on 88SC PICCs, then the corresponding key set is locked and all subsequent Authentication attempts will fail. If the AAC reaches the maximum count of 15 on 88RF PICCs, then the corresponding key set is locked and all subsequent Authentication attempts will fail.

If the AAC contents are corrupted, or are programmed with an undefined value, then the corresponding key set is locked and all subsequent Authentication attempts will fail. The AAC registers can always be read using the Read System Zone command.

Table J-8. Authentication Attempt Counter Coding for the Default Configuration of 88SC PICCs

AAC 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 J-9. Authentication Attempt Counter Coding for the Extended Trials Allowed Configuration of 88SC PICCs

AAC 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.	

Table J-10. Authentication Attempt Counter Coding for 88RF PICCs

AAC Register	Description
$55	No Failed Attempts
$56	1 Failed Attempt
$59	2 Failed Attempts
$5A	3 Failed Attempts
$65	4 Failed Attempts
$66	5 Failed Attempts
$69	6 Failed Attempts
$6A	7 Failed Attempts
$95	8 Failed Attempts
$96	9 Failed Attempts
$99	10 Failed Attempts
$9A	11 Failed Attempts
$A5	12 Failed Attempts
$A6	13 Failed Attempts
$A9	14 Failed Attempts
$AA	15 Failed Attempts (LOCK)
All Other Values Are Not Supported.	

J.8 Authentication Activation

Authentication Communication Security is activated using the following Mutual Authentication procedure.

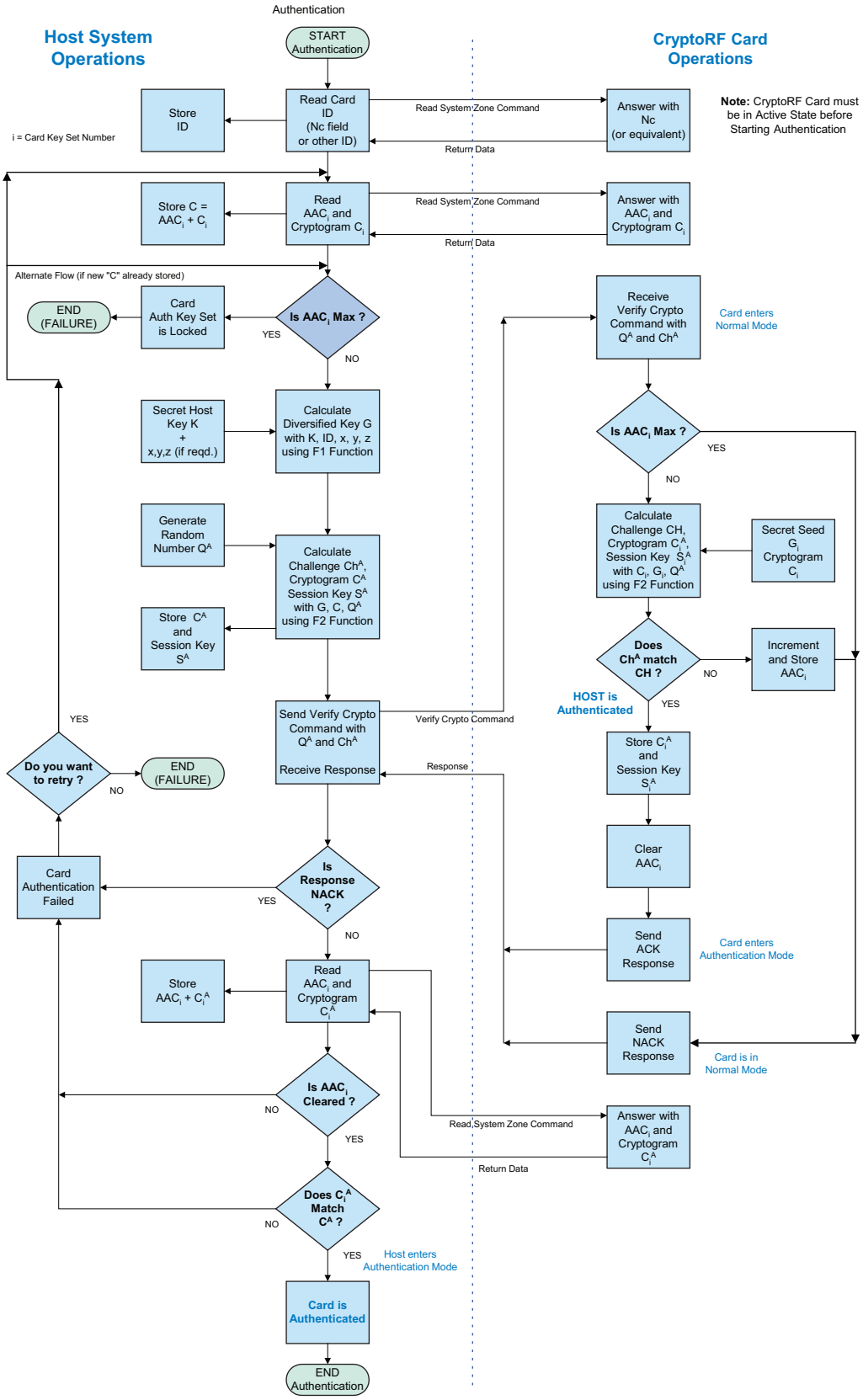
1. The Host reads the PICC ID from Nc (or another equivalent memory location) and calculates the diversified key matching the PICC Secret Seed G. G = F1(K, ID, x, y, z).
2. The Host reads AAC_i and C_i from card.
3. The Host generates a Random Number Q^A and calculates challenge CH^A and other parameters with the cryptographic engine: $[CH^A, C^A, S^A] = F2(G, C, Q^A)$.
4. The Host Sends Verify Crypto Command with Key Index $0i: Verify Crypto ($0i, Q^A, CH^A).
5. The PICC calculates challenge CH and other parameters using Q^A from the host with the cryptographic engine: $[CH, C_i^A, S_i^A] = F2(G_i, C_i, Q^A)$.
6. The PICC compares the internally calculated challenge CH to the value received from the host. If $CH = CH^A$ then the host is authenticated and the card writes the calculated values of C_i^A to the C_i register and S_i^A to the Si register. The AAC_i is cleared, Authentication Communication Security mode is activated, and an ACK response is returned to the host.
7. The Host reads the new AAC_i and C_i^A from C_i register of the PICC and compares it to the calculated C^A from Step 3. If $C^A = C_i^A$ then the card is authenticated. The Mutual Authentication procedure is complete.

The Secret Seed G_i value in the PICC never changes after it is locked at personalization. The AAC_i, and C_i registers are written (by the PICC) each time a Verify Crypto command is received by the PICC. The S_i register is written (by the PICC) each time the Mutual Authentication procedure succeeds.

If the Host receives a NACK response from the PICC, then the Mutual Authentication procedure can be retried starting with step 2.

Figure J-4 shows the Mutual Authentication procedure as a flowchart.

Figure J-4. Mutual Authentication Procedure



J.8.1 Key Index

The Key Index byte of the Verify Crypto command selects the Key Set that the PICC uses to perform the Mutual Authentication procedure.

Table J-11. Key Index coding for the Verify Crypto command for Mutual Authentication

Key Index	Key
$00	Secret Seed G_0
$01	Secret Seed G_1
$02	Secret Seed G_2
$03	Secret Seed G_3

J.9 Set User Zone and Checksums

The Mutual Authentication procedure can be performed before or after the Set User Zone command is sent. It is not necessary to repeat the Mutual Authentication procedure when changing User Zones unless the new User Zone requires a different Key Set. If Authentication Communication Security is activated and the application later selects a User Zone that does not require Authentication, the PICC will remain in Authentication Communication Security mode and all of the Authentication mode requirements will continue to apply.

When Authentication Communication Security is active the Host must supply a correct cryptographic checksum when writing data to a User Zone. This is true even if the User Zone Access Register does not require Authentication for access to the zone.

J.10 Passwords

When Authentication Communication Security is active Passwords are encrypted during communications. The Host is required to encrypt the three password bytes when sending the Check Password command. The PICC encrypts any password bytes that are accessed with the Read System Zone command. The Host is required to encrypt any password bytes when sending the Write System Zone command.

J.11 Deactivating Authentication Communication Security

Once activated, the PICC will remain in Authentication Communication Security mode until a security error occurs, a new Verify Crypto command is received, RF power is removed, or a DESELECT command or IDLE command is received.

In some applications it is necessary to deactivate Authentication Communication Security so that data can be written to a User Zone that has open read/write access without the necessity of computing a cryptographic checksum. While there are several possible ways to reset the cryptographic engine and exit the Authentication Communication Security mode, it is recommended that the Send Checksum command be used for this purpose.

If the PICC receives a Send Checksum command containing an incorrect checksum, the PICC resets the cryptographic engine, returns to Normal Communication mode, and returns a NACK response to the host. The AAC_i register is not incremented by the PICC when a bad checksum is received, so there is no penalty for using Send Checksum to exit Authentication mode.

Appendix K Using Encryption Communication 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 Encryption Communication Security on a User Zone restricts access to the data to users with knowledge of the Authentication key.

K.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 Communication Security mode encrypts only passwords. Encryption Communication Security mode encrypts both user data and passwords. The default communication mode is Normal mode.

Table K-1. CryptoRF Communication Security Options

Communication Mode	User Data	System Data	Passwords
Normal	Clear	Clear	Clear
Authentication	Clear	Clear	Encryption
Encryption	Encryption	Clear[(1)]	Encryption

Note: 1. 88RF PICCs support an encryption option for programming secrets. See Appendix F.

Encryption Communication Security is activated by performing Mutual Authentication between the Host system and the PICC using the Verify Crypto command, followed by the Encryption Activation procedure. Once activated, the PICC will remain in Encryption mode until a security error occurs, a new Verify Crypto command is received, RF power is removed, or a DESELECT command or IDLE command is received.

K.2 Encryption Security Options [88SC]

Encryption Communication Security for a User Zone is enabled by programming the Access Register (AR) and Password Register (PR) for the zone. The Communication Security Mode (M) bits [AM1, AM0, ER] of the Access Register determine the Communication Security requirements for the User Zone. The Password Register determines which Key Set is used to access the User Zone. Configuration of the AR and PR registers is described in Appendix H.

Table K-2. Selecting Encryption Using the Communication Security Mode Bits of the Access Register

AM1	AM0	ER	Communication Security Mode	Auth. Key (AK)	Pgm-Only Key (POK)
1	1	0	Encryption for Read / Write	Read / Write Access	N/A
1	1	1	No Authentication or Encryption Required	N/A	N/A

Table K-2 shows the one CryptoRF Encryption Communication Security option for 88SC PICCs, plus the default setting. By default M = 111b, and no Authentication or Encryption Activation is required to access the user memory.

K.2.1 M = 110b Security – Encryption for Read/Write

When M = 110b, Encryption is required for Read or Write access to the User Zone. If Encryption Activation is performed with the key identified in the AK bits of the Password Register, then Read/Write access is granted to the User Zone. A checksum is required for write operations.

K.3 Encryption Security Options [88RF]

Encryption Communication Security for a User Zone is enabled by programming the Access Register (AR) and Key Register (KR) for the zone. The Communication Security Mode (M) bits of the Access Register determine the Communication Security requirements for the User Zone. The Key Register determines which Key Set(s) are used to access the User Zone. Configuration of the AR and KR registers is described in Appendix H.

Table K-3. Selecting Encryption Using the Communication Security Mode Bits of the Access Register

M2	M1	M0	Communication Security Mode	Primary Key (PK)	Read-Only Key (ROK)
0	1	0	Authentication for Read/Encryption for Write	Read / Write Access	Read Access
1	0	0	Encryption for Write	Read / Write Access	N/A
1	1	0	Encryption for Read / Write	Read / Write Access	Read Access
1	1	1	No Authentication or Encryption Required	N/A	N/A

Table K-3 shows the three Encryption Security options for 88RF PICCs, plus the default setting. By default M = 111b, and no Authentication or Encryption Activation is required to access the user memory.

K.3.1 M = 010b Security - Authentication for Read / Encryption for Write

When M = 010b, Authentication is required for Read access to the User Zone. Encryption Activation is required for Write Access to the User Zone. If Authentication is performed with the key identified in the ROK bits of the Key Register, then Read-Only access is granted to the User Zone. If Encryption Activation is performed with the key identified in the PK bits of the Key Register, then Read/Write access is granted to the User Zone. A checksum is required for write operations.

The M = 010b mode is a new feature in 88RF PICCs. This mode is not available in 88SC devices.

K.3.2 M = 100b Security - Encryption for Write

When M = 100b Encryption is required for Write access to the User Zone. If Encryption Activation is performed with the key identified in the PK bits of the Key Register, then Read/Write access is granted to the User Zone. Read-Only access does not require Authentication or Encryption Activation. A checksum is required for write operations.

The M = 100b mode is a new feature in 88RF PICCs. This mode is not available in 88SC devices.

K.3.3 M = 110b Security — Encryption for Read/Write

When M = 110b Encryption is required for Read or Write access to the User Zone. If Encryption Activation is performed with the key identified in the PK bits of the Key Register, then Read/Write access is granted to the User Zone. If Encryption Activation is performed with the key identified in the ROK bits of the Key Register, then Read-Only access is granted to the User Zone. A checksum is required for write operations.

If the PK and ROK bits of the Key Register select the same Key Set, then the Read-Only function is effectively disabled. Encryption Activation of 88RF PICCs with the PK key results in behavior identical to 88SC devices. The Read-Only function is not supported by 88SC devices.

K.4 The Password Register [88SC]

The Password Registers are used to select the Key Sets for Authentication or Encryption Communication Security on 88SC PICCs. Any Key Set can be used with any User Zone by programming the Password Register for the User Zone with the appropriate AK and POK values. One Key Set can be used with any number of User Zones.

Figure K-1. Definition of the User Zone Password Registers on 88SC PICCs

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

The Authentication Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register bits determine the Communication Security mode associated with the AK bits.

Table K-4. Coding of the Authentication Key Set Select Bits for CryptoRF Communication Security

AK1	AK0	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

The Program-Only Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register bits determine the Communication Security mode associated with the POK bits. The POK bits are only used in Dual Access Authentication mode.

Table K-5. Coding of the Program-Only Key Set Select Bits for CryptoRF Communication Security

POK1	POK0	Authentication Key
0	0	Secret Seed G_0
0	1	Secret Seed G_1
1	0	Secret Seed G_2
1	1	Secret Seed G_3

K.5 The Key Register [88RF]

The Key Registers are used to select the Key Sets for Authentication or Encryption Communication Security on 88RF PICCs. Any Key Set can be used with any User Zone by programming the Key Register for the User Zone with the appropriate PK and ROK values. One Key Set can be used with any number of User Zones.

Figure K-2. Definition of the Key Registers on 88RF PICCs

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
PK1	PK2	ROK1	ROK2	RFU	PW2	PW1	PW0	
1	1	1	1	1	1	1	1	Default Value

The Primary Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register M bits determine the Communication Security mode associated with the PK bits.

Table K-6. Coding of the Primary Key Set Select Bits for CryptoRF Communication Security

PK1	PK2	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

The Read-Only Key Set selection bits control the key set assigned to a User Zone for communication security. The Access Register M bits determine the Communication Security mode associated with the ROK bits. For some Communication Security modes the ROK register bits are not used.

Table K-7. Coding of the Read-Only Key Set Select Bits for CryptoRF Communication Security

ROK1	ROK2	Authentication Key	Encryption Key
0	0	Secret Seed G_0	Session Key S_0
0	1	Secret Seed G_1	Session Key S_1
1	0	Secret Seed G_2	Session Key S_2
1	1	Secret Seed G_3	Session Key S_3

K.6 Key Sets

CryptoRF has four Key Sets. Each Key Set is associated with four registers in the Configuration Memory. The Authentication Key is stored in the Secret Seed G_i register. The Authentication Attempt Counter for Secret Seed G_i is stored in the AAC_i register. The Cryptogram C_i register is used during Authentication Activation and Encryption Activation procedures to store the response to the Host challenge. The Session Key S_i register is used to store the Encryption Activation key.

Figure K-3. Partial Configuration Memory Map Showing the Key Set Registers

	$0	$1	$2	$3	$4	$5	$6	$7	
$50	AAC_0	Cryptogram C_0							Cryptography
$58	Session Encryption Key S_0								
$60	AAC_1	Cryptogram C_1							
$68	Session Encryption Key S_1								
$70	AAC_2	Cryptogram C_2							
$78	Session Encryption Key S_2								
$80	AAC_3	Cryptogram C_3							
$88	Session Encryption Key S_3								
$90	Secret Seed G_0								Secret
$98	Secret Seed G_1								
$A0	Secret Seed G_2								
$A8	Secret Seed G_3								

Figure K-3 shows the portion of the Configuration Memory that contains the Key Set registers. The registers shaded in green can always be read, but cannot be written after personalization. The registers shaded in blue cannot be written or read after personalization.

Note: All of the Security Fuses must be programmed during personalization for the device secrets to be secure.

Key Set i uses registers AAC_i, C_i, G_i and S_i. If AAC_i is locked, the Key Set i is permanently disabled and any User Zone requiring Key Set i for Authentication or Encryption Activation will no longer be accessible.

K.6.1 Changing Keys

The Secret Seeds cannot be modified after the Security Fuses are programmed during personalization. The AAC registers cannot be re-written after the Security Fuses are programmed either. This is true even if the SME option in the DCR register is enabled.

K.7 AAC Registers

The Authentication Attempt Counters contain a value which indicates how many unsuccessful Authentication and Encryption Activation attempts have been made using the Key Index of the corresponding Secret Seed and Session Encryption Key. Table K-8, Table K-9, and Table J-10 show coding of the AAC register. If the AAC reaches the maximum count of four or eight on 88SC PICCs, then the corresponding key set is locked and all subsequent Authentication attempts will fail. If the AAC reaches the maximum count of 15 on 88RF PICCs, then the corresponding key set is locked and all subsequent Authentication attempts will fail.

If the AAC contents are corrupted, or are programmed with an undefined value, then the corresponding key set is locked and all subsequent Authentication attempts will fail. The AAC registers can always be read using the Read System Zone command.

Table K-8. Authentication Attempt Counter Coding for the Default DCR Configuration on 88SC PICCs

AAC 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 K-9. Authentication Attempt Counter Coding for the Extended Trials Allowed DCR Configuration on 88SC PICCs

AAC 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.	

Table K-10. Authentication Attempt Counter Coding for 88RF PICCs

AAC Register	Description
$55	No Failed Attempts
$56	1 Failed Attempt
$59	2 Failed Attempts
$5A	3 Failed Attempts
$65	4 Failed Attempts
$66	5 Failed Attempts
$69	6 Failed Attempts
$6A	7 Failed Attempts
$95	8 Failed Attempts
$96	9 Failed Attempts
$99	10 Failed Attempts
$9A	11 Failed Attempts
$A5	12 Failed Attempts
$A6	13 Failed Attempts
$A9	14 Failed Attempts
$AA	15 Failed Attempts (LOCK)
All Other Values Are Not Supported.	

K.8 Encryption Activation

Authentication Activation must be performed prior to Encryption Activation. The Mutual Authentication is performed in steps one thru seven, and Encryption Activation in steps eight thru eleven of the following procedure.

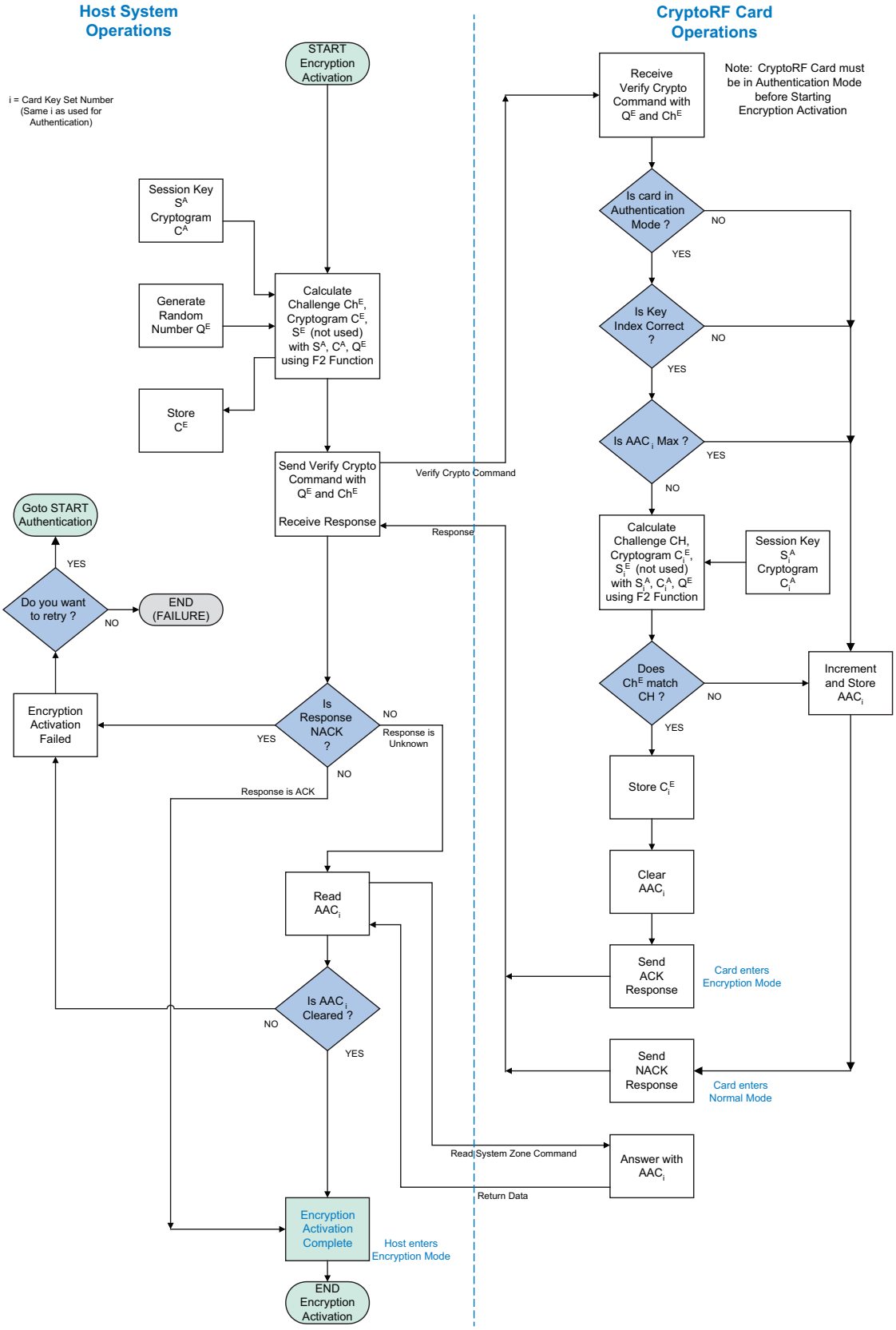
1. The Host reads the PICC ID from Nc (or another equivalent memory location) and calculates the diversified key matching the PICC Secret Seed G. G = F1(K, ID, x, y, z).
2. The Host reads AACi and Ci from card.
3. The Host generates a Random Number QA and calculates challenge CHA and other parameters with the cryptographic engine: [CHA, CA, SA] = F2(G, C, QA)
4. The Host Sends Verify Crypto Command with Key Index $0i: Verify Crypto ($0i, QA, CHA)
5. The PICC calculates challenge CH and other parameters using QA from the host with the cryptographic engine: [CH, CiA, SiA] = F2(Gi, Ci, QA)
6. The PICC compares the internally calculated challenge CH to the value received from the host. If CH = CHA then the host is authenticated and the card writes the calculated values of CiA to the Ci register and SiA to the Si register. The AACi is cleared, Authentication Communication Security mode is activated, and an ACK response is returned to the host.
7. The Host reads the new AACi and CiA from Ci register of the PICC and compares it to the calculated CA from Step 3. If CA = CiA, then the card is authenticated. The Mutual Authentication procedure is complete.
8. The Host generates a Random Number QE and calculates challenge CHE and other parameters with the cryptographic engine: [CHE, CE] = F2(SiA, CiA, QE).
9. The Host Sends Verify Crypto Command with Key Index $1i: Verify Crypto ($1i, QE, CHE).
10. The PICC calculates challenge CH and other parameters using QE from the host with the cryptographic engine: [CH, CiE] = F2(SiA, CiA, QE).
11. The PICC compares the internally calculated challenge CH to the value received from the host. If CH = CHE, then the host is authenticated and the card writes the calculated value of CiE to the Ci register. The AACi is cleared, Encryption Communication Security mode is activated, and an ACK response is returned to the host.

The Secret Seed G_i value in the PICC never changes after it is locked at personalization. The AAC_i, and C_i registers are written (by the PICC) each time a Verify Crypto command is received by the PICC. The S_i register is written (by the PICC) each time the Mutual Authentication procedure succeeds.

If the Host receives a NACK response from the PICC, then the Mutual Authentication procedure can be retried starting with step 2.

Figure J-4 shows the Authentication Activation procedure as a flowchart. Figure K-4 shows the Encryption Activation procedure as a flowchart.

Figure K-4. Encryption Activation Procedure



K.8.1 Key Index

The Key Index byte of the Verify Crypto command selects the Key Set that the PICC uses to perform the Mutual Authentication and Encryption Activation procedure.

Table K-11. Key Index Coding for the Verify Crypto Command

Key Index	Key
$00	Secret Seed G0
$01	Secret Seed G1
$02	Secret Seed G2
$03	Secret Seed G3
$10	Session Encryption Key S0
$11	Session Encryption Key S1
$12	Session Encryption Key S2
$13	Session Encryption Key S3
All Other Values Are Not Supported.	

K.9 Set User Zone and Checksums

The Mutual Authentication and Encryption Activation procedures can be performed before or after the Set User Zone command is sent. It is not necessary to repeat the Mutual Authentication and Encryption Activation procedure when changing User Zones unless the new User Zone requires a different Key Set. If Encryption Communication Security is activated and the application later selects a User Zone that does not require Encryption, the PICC will remain in Encryption Communication Security mode, User Zone data will be encrypted, and all of the Encryption mode requirements will continue to apply.

When Encryption Communication Security is active the Host must supply a correct cryptographic checksum when writing data to a User Zone. This is true even if the User Zone Access Register does not require Encryption for access to the zone.

K.10 Passwords

When Encryption Communication Security is active Passwords are encrypted during communications. The Host is required to encrypt the three password bytes when sending the Check Password command. The PICC encrypts any password bytes that are accessed with the Read System Zone command. The Host is required to encrypt any password bytes when sending the Write System Zone command.

K.11 Deactivating Encryption Communication Security

Once activated, the PICC will remain in Encryption Communication Security mode until a security error occurs, a new Verify Crypto command is received, RF power is removed, or a DESELECT command or IDLE command is received.

In some applications, it is necessary to deactivate Encryption Communication Security so that data can be written to a User Zone that has open read/write access without the necessity of computing a cryptographic checksum. While there are several possible ways to reset the cryptographic engine and exit the Encryption Communication Security mode, it is recommended that the Send Checksum command be used for this purpose.

If the PICC receives a Send Checksum command containing an incorrect checksum, the PICC resets the cryptographic engine, returns to Normal Communication mode, and returns a NACK response to the host. The AAC_i register is not incremented by the PICC when a bad checksum is received, so there is no penalty for using Send Checksum to exit Authentication or Encryption mode.

Appendix L 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 Host during a transaction, it is not controlled by any configuration register.

L.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.

L.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 it should be activated only for critical data write operations.

Figure L-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.

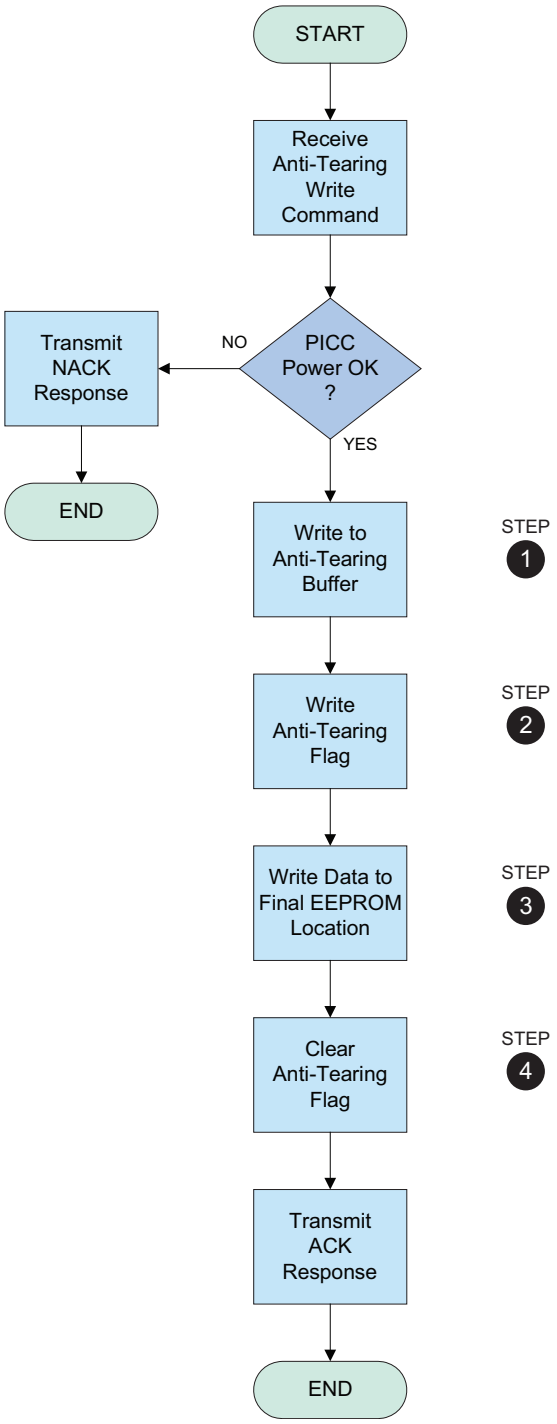
If power is interrupted before Step 2 is completed, then the write operation fails; the EEPROM contents are unchanged, and the Anti-Tearing Flag is not set to indicate an anti-tearing write is in progress. If power is interrupted after Step 2 is complete, then the Anti-Tearing flag is set; when the PICC 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.

Table L.3 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 L-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.

Figure L-1. CryptoRF Anti-Tearing Write Process



L.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 eight 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 eight bytes of data, the net result is an increase in the transaction time of only 5ms. When large amounts of data are written, the increase in transaction time is significant. Writing the entire 128 byte User Zone on AT88RF04C takes 155ms with anti-tearing, but only 47ms without anti-tearing. Writing the entire 256 byte User Zone on AT88SC3216CRF takes 292ms with anti-tearing, but only 54ms without anti-tearing.

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

CryptoRF Part Number	Write Characteristics	
	Standard Write	Anti-Tearing Write
AT88RF04C	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

L.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 L-3. CryptoRF Family Write Endurance with Anti-Tearing

Parameter	Min	Typical	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.

L.5 Activating Anti-Tearing

Anti-Tearing can be used for either User Zone or Configuration Memory writes on 88SC PICCs. Anti-Tearing is available for User Zone writes only on 88RF PICCs. 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 seven 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 seven in the PARAM byte set to 0b. All subsequent Write User Zone commands will automatically use the normal write process.

Table L-4. Definition 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 on 88SC PICCs, the anti-tearing function is controlled by the PARAM byte of the Write System Zone command. Table L-2 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.

Figure L-2. PARAM Byte Options for the Write System Zone Command for 88SC PICCs

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.				

Appendix M 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 appendix describes the requirements for programming the polling registers for operation with ISO/IEC 14443 compliant readers and systems.

M.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 Appendix N 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 identify 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.

M.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 M-1 and Figure M-2). The values stored in the following registers are used during anticollision: PUPI, APP, RBmax, and AFI.

Figure M-1. Memory Map of Anticollision Registers in the System Zone of 88SC PICCs.

<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">CMC</td></tr>
</table>

Figure M-2. Memory Map of Anticollision Registers in the System Zone of 88RF PICCs.

<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="2">CMC</td><td colspan="2">HWR</td></tr>
</table>

The REQB/WUPB polling command and response are shown in Figure M-3 with color-coding which matches Figure M-1 and Appendix M-2. 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 M-3. 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
		APP1	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.

PUPI: Pseudo Unique PICC Identifier

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.

APP: Application Data

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 Table M-1); this byte can be redefined by the card manufacturer if desired. APP may be set to any value.

Table M-1. Default Value of APP 3 Byte. This Register Can Be Changed.

Device Number	Density Code
AT88RF04C	$22
AT88SC0808CRF	$33
AT88SC1616CRF	$44
AT88SC3216CRF	$54
AT88SC6416CRF	$64

RBmax: Receive Buffer Max Code

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 four bits and the code for the maximum frame size supported by the card in the upper four 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 Table M-2.

Table M-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 four bits of ATQB Protocol Byte 2 in a register and echo it back to a selected PICC in the lower four bits of ATTRIB Parameter Byte 3. CryptoRF will not accept an ATTRIB command with a non-zero value in Parameter Byte 3.

Note: Intelligent PCDs will reject invalid ATQB responses and will not send invalid ATTRIB commands.

Table M-3. Default Value of RBmax. This Register Should Not Be Changed.

Device Number	RBmax Code
AT88RF04C	$10
AT88SC0808CRF	$10
AT88SC1616CRF	$10
AT88SC3216CRF	$30
AT88SC6416CRF	$30

AFI: Application Family Identifier

This eight 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 four bits are the application family and the lower four bits are the subfamily. The ISO/IEC 14443 Part 3 Type B application family definitions are shown in Table M-4. 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 M-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, Electronic Purse…
$3	“Y”	Identification	Access Control…
$4	“Y”	Telecom	Telephony, GSM…
$5	“Y”	Medical	
$6	“Y”	Multimedia	Internet Services…
$7	“Y”	Gaming	
$8	“Y”	Data Storage	Portable Files…
$9 – $D	“Y”	RFU	not currently defined by 14443-3
$E	“Y”	Travel Documents (MRTD)	Y=$1 Passport, Y=$2 Visa, Y=$3 to $F *RFU*
$F	“Y”	RFU	not currently defined by 14443-3

Note: 1. “Y” = $1 to $5

The PICC compares the AFI register with the AFI value received in the REQB or WUPB polling command using the matching criteria defined in ISO/IEC 14443 Part 3. Table M-5 shows the AFI matching criteria.

Table M-5. 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 Subfamilies
“X”	$0	All Subfamilies of Family “X”
“X”	“Y”	Only Subfamily “Y” of Family “X”
$0	“Y”	Proprietary Subfamily “Y” Only

Notes: 1. “Y” = $1 to $F
2. “X” = $1 to $F

M.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 appendix.

Appendix N Understanding Anticollision

This section of the specification and the flow chart in Figure N-1 describe the anticollision procedure for the CryptoRF family. The command and response definitions are detailed in Section 6. “Anticollision Command Definitions” on page 12. For additional information on the anticollision command coding, see Section 7 of ISO/IEC 14443 Part 3 or the Atmel Application Note, *Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards*.

When the PICC enters the 13.56MHz RF field of the host reader (PCD), it performs a Power-On Reset (POR) 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 one to “N”; if “R” = 1 then the PICC responds with ATQB. If “R” is greater than one, 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.

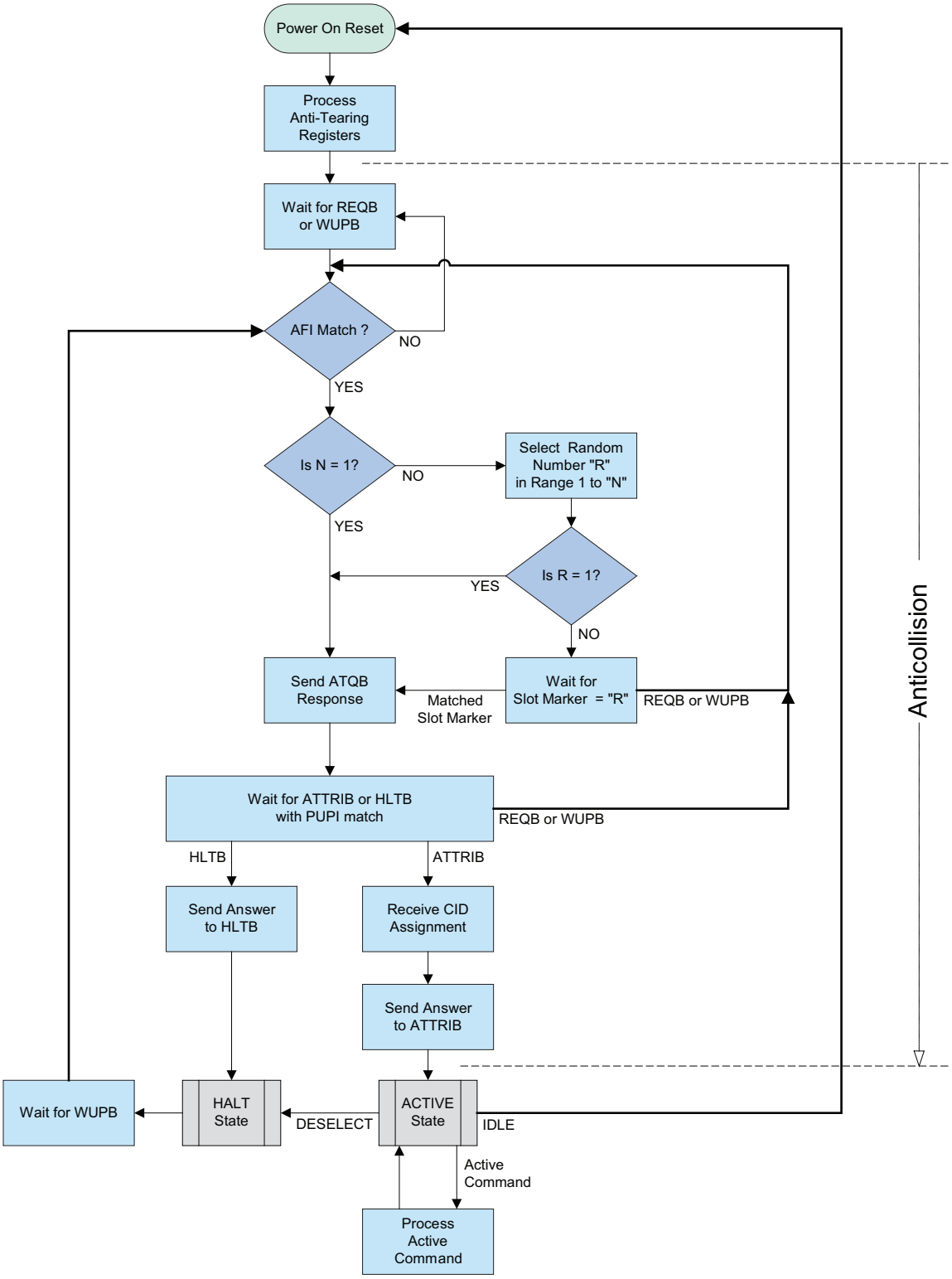
The ATQB response contains a PUPI card serial number which is used to direct commands to a specific PICC during the anticollision process. When the PCD receives an ATQB response, it can respond with a matching HLTB command to Halt the PICC, or it can respond with a matching ATTRIB command to assign a 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: ISO/IEC 14443 Part 3 describes two anticollision options for Type B PICCs; the Timeslot option has been implemented in the CryptoRF family.

Figure N-1. Anticollision and State Transition Flow Chart



Appendix O The ISO/IEC 14443 Type B RF Signal Interface

O.1 RF Signal Interface

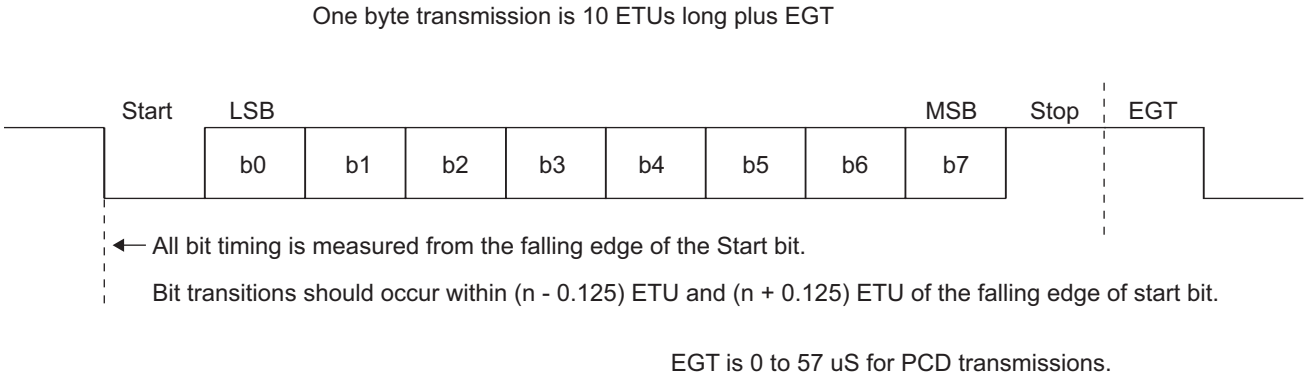
The CryptoRF communications interface is compliant with the ISO/IEC 14443 Part 2 and Part 3 requirements for Type B. Type B signaling utilizes ten percent amplitude modulation of the RF field for communication from the reader to the card with NRZ encoded data. Communication from card to reader utilizes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

O.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 O-1. The stop bit, start bit, and each data bit are each one elementary time unit (ETU) in length (9.4395µs).

Each byte transmission consists of a Start bit, eight 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 57µs for data transmitted by the PCD. EGT for data transmitted by the CryptoRF PICC is programmed to either zero or two 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 O-1. Byte transmission format requirements for type B communications.

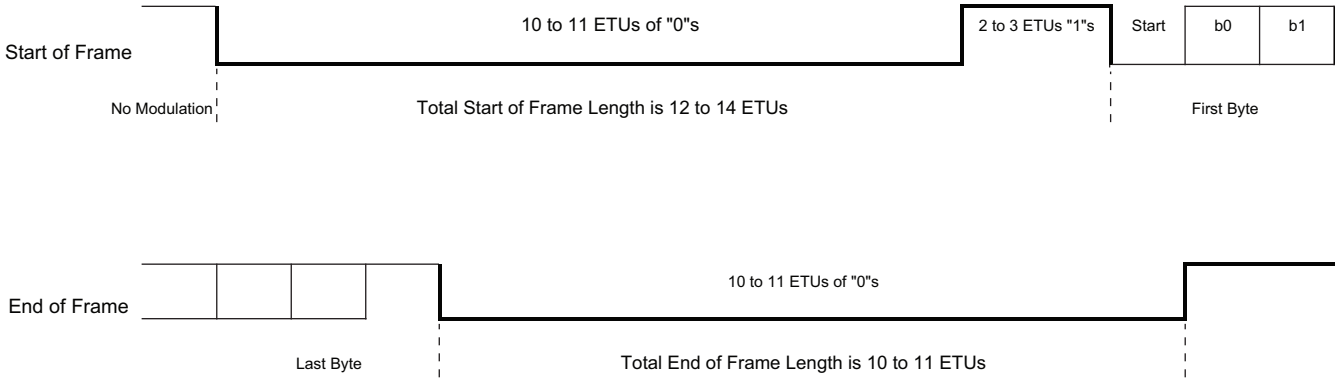


Despite the fact that data transmissions occur LSB first, all of the commands, data, and CRC bytes in ISO/IEC 14443 and in this specification are listed in the conventional manner, with MSB on the left and LSB on the right.

O.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 O-2.

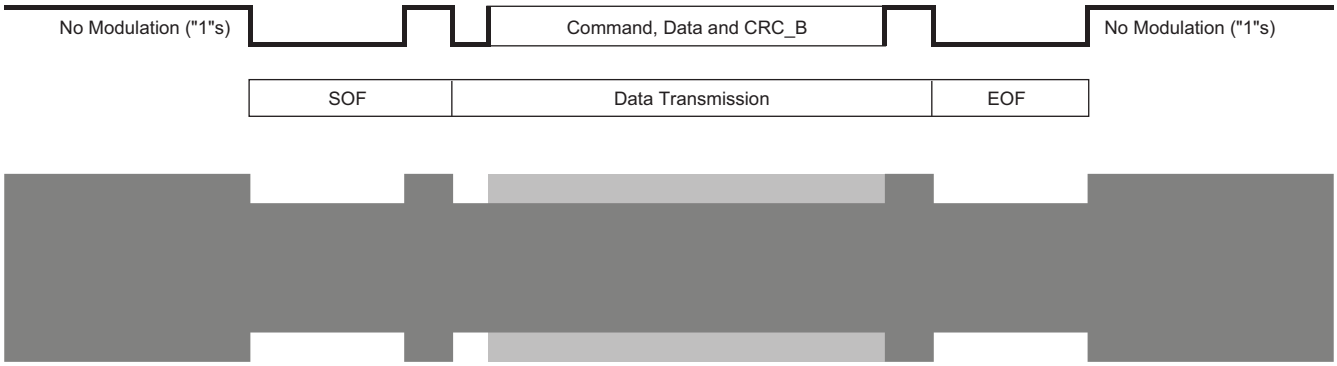
Figure O-2. Start of Frame (SOF) and End of Frame (EOF) Format Requirements



O.4 Reader Data Transmission

The unmodulated 13.56MHz 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 two byte CRC_B, and the EOF.

Figure O-3. Format of a Frame Transmitted by the Reader to the Card

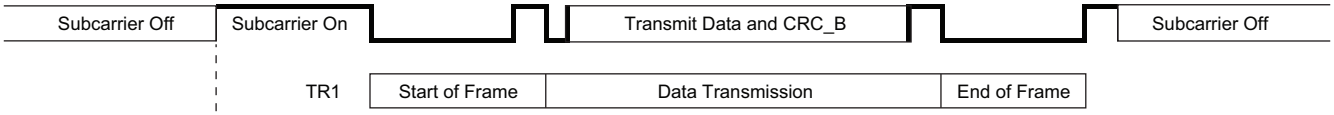


O.5 Card Data Transmission

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 two byte CRC_B, and the EOF. The subcarrier is turned off no later than two ETUs after the EOF. Figure O-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 1 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.

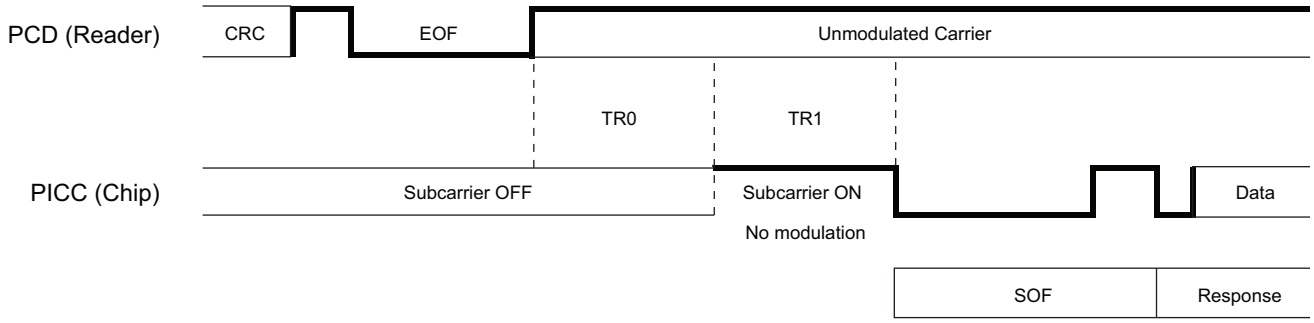
Figure O-4. Format of a Frame Transmitted by the PICC to the Reader



O.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 eight 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 O-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 Appendix Q See Appendix P 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.

O.7 CRC Error Detection

A two 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 O-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 O-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.

O.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.

Appendix P 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 Appendix all of the RF requirements are summarized, and antenna size related parameters are identified.

P.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.

P.1.1 AC Characteristics

Table P-1. CryptoRF PICC Characteristics [Not PICC Antenna Size Dependent][(1)]

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 (fc/128)	9.4346	9.4395	9.4444	µs	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 (ATQB Response Only)	8		10	ETU	14443-3 7.1.6
TR0	Guard Time (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	

Note: 1. Nominal values at 25°C. Values are based on characterization and are not tested.

The RF Interface characteristics of the CryptoRF family are listed in Table Q-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 Q-1 are guaranteed by design. Appendix O contains illustrations of the RF interface timing parameters.

P.2 Reader Requirements

Table P-2. ISO/IEC 14443 Reader Requirements [Not PICC Antenna Size Dependent][(1)]

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 (fc /128)	9.4346	9.4395	9.4444	µs	14443-2 9.1.1
EGT	Extra Guard Time (PCD to PICC Communication)	0		57	µs	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

Note: 1. Nominal values at 25° C.

The CryptoRF family has been designed to operate with an ISO/IEC 14443 Type B compliant PCDs meeting the requirements listed in Table P-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 P-2 are not PICC antenna size dependent.

P.3 PICC Antenna Size Dependent Specifications

Table P-3. Antenna Size Dependent Characteristics [ID-1 PICC Antennas Only][(1)]

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	14443-1 4.3.5
	Load Modulation Amplitude at Hmin (1.5A/m rms)	18.45			mV peak	14443-2 9.2.2 (test per 10373-6)
	Load Modulation Amplitude at Hmin (7.5A/m rms)	2.68			mV peak	

Note: 1. Nominal values at 25°C. Values are based on characterization and are not tested.

The specifications in Table Q-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 3000mm^2 area of a typical ID-1 antenna. The Hmin and Hmax limits of 1.5A/m rms and 7.5A/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 7.5A/m rms. An ID-1 PICC is required to survive continuous exposure to a 10A/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.

P.4 Specifications for Other Antenna Sizes

The specifications in Table Q-3 cannot be applied directly to PICCs with larger or smaller antennas. The characteristics in Table P-1 and Table P-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 3000mm2 as the ID-1 antenna area).

Note: 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 6000mm^2 PICC Antenna. 3000/6000 = 0.5 The minimum operating magnetic field (Hmin) is 1.5 x 0.5 = 0.75A/m rms. The maximum operating magnetic field (Hmax) is 7.5 x 0.5 = 3.75A/m rms. This PICC can be expected to survive exposure to a non-operating magnetic field of 10 x 0.5 = 5.0A/m rms.

Example 2: Guidelines for operation of a 1000 mm^2 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 30A/m rms may be hazardous to your health.

P.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 P-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 eight percent and fourteen percent.

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 P-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

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

P.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 85.6mm by 53.98mm and 0.76mm 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 72mm x 42mm with four concentric turns. The antenna trace width and spacing are both 0.5mm 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 its antenna located entirely within a zone defined by two rectangles centered in the ID-1 dimensions. The external rectangle is 81mm by 49mm. The internal rectangle is 64mm x 34mm, with a 3mm 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.

P.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.

Appendix Q Transaction Time

Q.1 Command Response Times [88SC]

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 Q-1. Command Response Timing for the CryptoRF Command Set for 88SC PICCs[1]

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 with 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 with 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

Note: 1. Nominal values at 25° C. Values are based on characterization and are not tested.

Q.2 Command Response Times [88RF]

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 Q-2. Command Response Timing for the CryptoRF Command Set for 88RF PICCs[1]

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 16 Bytes	2424	2700	97
Write User Zone with Anti-Tearing 8 bytes	7087	8000	97
Write User Zone Authentication Mode 16 bytes	2424	2700	97
Write User Zone Encryption Mode 16 bytes	2424	2700	97
Write System Zone 16 bytes	2424	2700	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

Note: 1. Nominal values at 25° C. Values are based on characterization and are not tested.

Q.3 Transaction Times [88SC]

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 Q-3. Transaction Time for the CryptoRF Command Set for 88SC PICCs[1]

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 with 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 16 bytes	4.8	5.8
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

Note: 1. Nominal values at 25° C. Values are based on characterization and are not tested.

Q.4 Transaction Times [88RF]

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 Q-4. Transaction Time for the CryptoRF Command Set for 88RF PICCs[1]

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	3.6	4.1
Write User Zone 8 bytes	4.5	4.9
Write User Zone with AT 8 bytes	9.5	11.0
Write User Zone 16 bytes	5.6	6.1
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	3.6	4.1
Write System Zone 8 bytes	4.5	4.9
Write System Zone 16 bytes	5.6	6.1
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

Note: 1. Nominal values at 25° C. Values are based on characterization and are not tested.

Appendix R 88RF PICC Backward Compatibility

88RF PICCs can be configured to operate in the majority of applications developed for 88SC PICCs. Customers migrating from 88SC devices to 88RF devices may be required to change their application software if they are using functions identified in this appendix.

R.1 Error Handling

When a command packet containing errors is received by an 88SC or 88RF PICC, the status code returned in the NACK response is the first error detected by the logic. The status code returned by 88RF PICCs may be different from the status code returned by 88SC PICCs.

R.2 Security Options

The Access Register (AR) and Device Configuration Register (DCR) definitions for 88RF PICCs are not exactly the same as the 88SC PICC definitions. Some RFU bits have been assigned new functionality. The changes which impact backward compatibility are summarized here.

R.2.1 Program Only Mode

88RF PICCs allows the Program Only Mode in User Zone 1 only. Program Only Mode is not allowed in User Zones 0, 2, or 3. The Access Register PGO bit is RFU for registers AR0, AR2, and AR3.

R.2.2 Write Lock Mode

88RF PICCs do not support Write Lock Mode. The Access Register WLM bit is RFU.

R.2.3 Unlimited Checksum Read

88RF PICCs do not support Unlimited Checksum Reads. The Device Configuration Register UCR bit is RFU.

R.2.4 Extended Trials Allowed

The CryptoRF Device Configuration Register ETA bit is RFU. The 88RF PICC attempts limit is always 15; it is no longer configurable. [88SC PICCs allowed four or eight attempts.]

R.2.5 Dual Access Mode

88RF PICCs do not support Dual Access Mode. The CryptoRF Access Register bits which selected Dual Access Mode have been assigned to another communication security mode.

R.3 Attempt Counters

Both the Password Attempts Counters (PACs) and Authentication Attempts Counters (AACs) have been redesigned to allow 15 failed attempts before the Password or Key is locked. The coding of the PAC and AAC registers has been changed to support the increased attempts counts.

R.4 Checksums

The requirement to supply a valid checksum when performing a write in Encryption Communication mode and Authentication Communication mode is strictly enforced by 88RF PICCs. (88SC PICCs require a valid checksum if the Access Register security mode bits for the current User Zone require that Encryption Communication mode or Authentication Communication mode be active to write the User Zone. If Authentication or Encryption is not required, then 88SC PICCs do not always require that a valid checksum be supplied to perform a write.)

R.5 Personalization

The 88RF PICC fuse bit functionality has been changed to allow enhanced security during the device personalization process. See Appendix F and Appendix G for information.

Customers that do not program any of the security fuses until the end of the personalization process will not notice a difference when personalizing 88RF PICCs. 88RF PICCs act the same as 88SC PICCs when the security fuses are in the default state.

R.5.1 Write System Zone with Anti-Tearing

88RF PICCs do not support Anti-Tearing writes using the Write System Zone command. Attempts to activate this option will result in a NACK response.

R.5.2 Reserved Memory

88RF PICCs do not allow writes to registers identified in the Configuration Memory Map as reserved. Any attempts to write these registers will be NACKed. Attempts to read the Configuration Memory using a starting address which is a reserved byte will be NACKed.

R.5.3 OTP Memory

88RF PICCs have 25 bytes of OTP memory available for customer use in the Configuration Memory; 88SC PICCs have 27 bytes of OTP memory available for customer use. In 88RF PICCs bytes $0E and $0F are the read-only Hardware Revision Register (HWR); in 88SC PICCs these bytes are available for customer use.

Appendix S Ordering Information

S.1 CryptoRF with 4Kb of User Memory Configured as 4 Zones of 128 bytes Each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88RF04C-MR1G	R Module	82pF	Commercial (0°C to 70°C)
AT88RF04C-MX1G	MX1 RFID Tag, 13.0mm square		Commercial (-25°C to 70°C)
AT88RF04C-MVA1	MVA1 RFID Tag, 8.6mm x 18.1mm		
AT88RF04C-WA1	6mil wafer, 150.0mm diameter		Industrial (-40°C to 85°C)

S.2 CryptoRF with 8Kb of User Memory Configured as 8 Zones of 128 bytes Each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC0808CRF-MR1	R Module	82pF	Commercial (0°C to 70°C)
AT88SC0808CRF-MX1	MX1 RFID Tag, 13.0mm square		Commercial (-25°C to 70°C)
AT88SC0808CRF-MVA1	MVA1 RFID Tag, 8.6mm x 18.1mm		
AT88SC0808CRF-WA1	6mil wafer, 150.0mm diameter		Industrial (25°C to 85°C)

S.3 CryptoRF with 16Kb of User Memory Configured as 16 Zones of 128 bytes Each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC1616CRF-MX1	MX1 RFID Tag, 13.0mm square	82pF	Commercial (-25°C to 70°C)
AT88SC1616CRF-MVA1	MVA1 RFID Tag, 8.6mm x 18.1mm		
AT88SC1616CRF-WA1	6mil wafer, 150.0mm diameter		Industrial (25°C to 85°C)

S.4 CryptoRF with 32Kb of User Memory Configured as 16 Zones of 256 bytes Each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC3216CRF-MX1	MX1 RFID Tag, 13.0mm square	82pF	Commercial (-25°C to 70°C)
AT88SC3216CRF-MVA1	MVA1 RFID Tag, 8.6mm x 18.1mm		
AT88SC3216CRF-WA1	6mil wafer, 150.0mm diameter		Industrial (25°C to 85°C)

S.5 CryptoRF with 64Kb of User Memory Configured as 16 Zones of 512 bytes Each

Ordering Code	Package	Tuning Capacitor	Temperature Range
AT88SC6416CRF-MR1	R Module	82pF	Commercial (0°C to 70°C)
AT88SC6416CRF-MX1	MX1 RFID Tag, 13.0mm square		Commercial (-25°C to 70°C)
AT88SC6416CRF-MVA1	MVA1 RFID Tag, 8.6mm x 18.1mm		
AT88SC6416CRF-WA1	6mil wafer, 150.0mm diameter		Industrial (25°C to 85°C)

S.6 Package Types

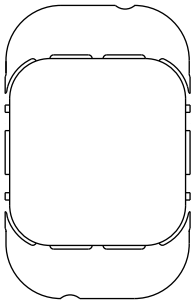
Package Type	Description
R Module	2-lead RF Smart Card Module, XOA2 style, on 35.0mm tape, Ag Finish, Green[(1)]
MX1 RFID Tag	13.0mm x 13.0mm Square Epoxy Glass RFID Tag on 35.0mm tape, Au Finish, Green[(1)]
MVA1 RFID Tag	8.6mm x 18.1mm Rectangular Epoxy Glass RFID Tag on 35.0mm tape, Au Finish, Green[(1)]

Notes: 1. Lead-free, halogen-free package. Exceeds RoHS requirements.

2. 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.

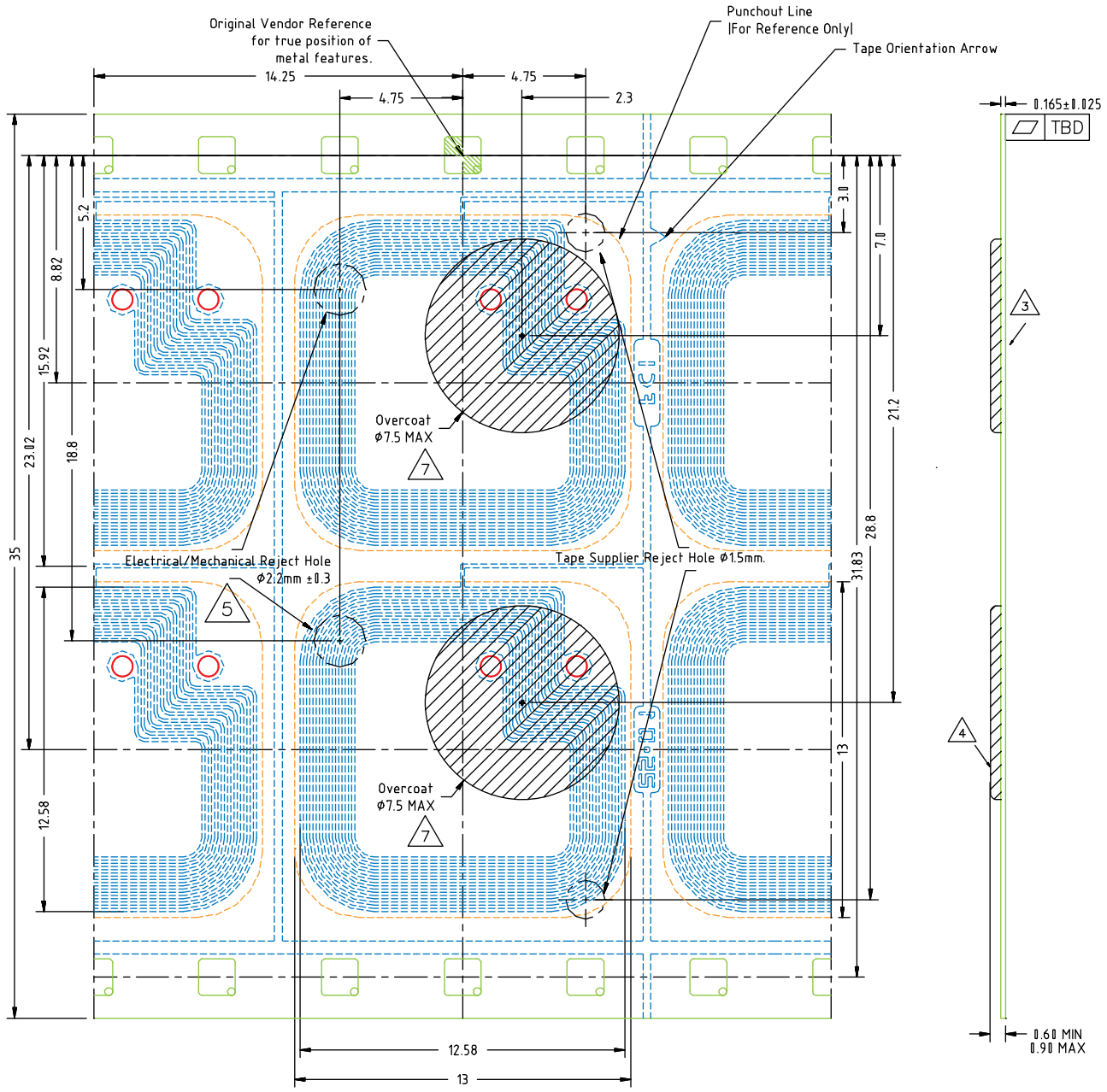
S.7 Packaging Information — Mechanical Drawings

S.7.1 Module R Package (XOA2 Style) — Ordering Code: AT88RFxxC-MR1G and AT88SCxxCRF-MR1

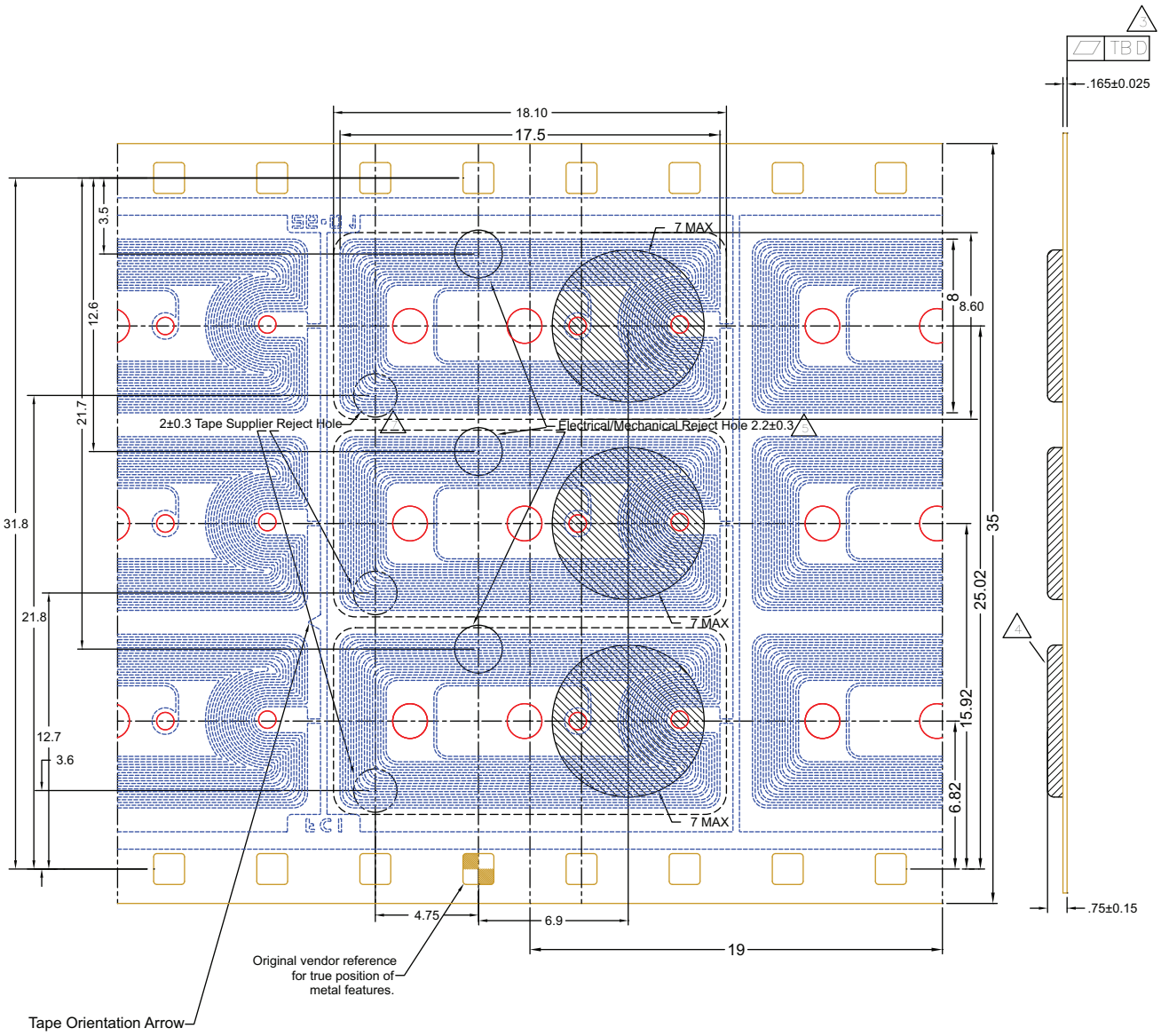


Module Size:	M5
Dimension:	5.06mm x 8.00mm
Glob Top:	Square – 4.8mm x 5.1mm
Thickness:	0.38mm
Pitch:	9.5mm

S.7.2 MX1 Epoxy Glass RFID Tag — Ordering Code: AT88RFxxC-MX1G and AT88SCxxCRF-MX1



S.7.3 MVA1 Epoxy Glass RFID Tag — Ordering Code: AT88RF04C-MVA1 and AT88SCxxCRF-MVA1



Appendix T Errata

T.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 41 bits of the register contain the Unique Serial Number, while the other 23 bits contain additional lot history information. Since this is a read-only register, these bits can be used by customers to uniquely identify a particular die for anticollision, authentication key diversification, or any other purpose required by the application.

Table T-1. Contents of UDSN (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.

Atmel reserves the right to modify the format of the contents of the UDSN register without notice; however, the UDSN register value is guaranteed to be unique for each die. The register name in the Configuration Memory Maps has been updated to Unique Die Serial Number in Revision B of this document to reflect this change.

T.2 Read User Zone command

As 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 User Zone during a read, then the address will roll-over to the first byte of the same User Zone.

T.3 Read User Zone command PARAM Codes [88RF]

The Read User Zone command accepts PARAM = $01, $02, $03 and interprets them as PARAM = $00. The Read User Zone command accepts PARAM = $81, $82, $83 and interprets them as PARAM = $80. In both cases, the read operation succeeds, when it should NACKed due to an invalid PARAM.

This error will be fixed in future products. Customers are advised that these PARAM values are not supported.

T.4 Status Codes [88RF]

In the response to each CryptoRF command the PICC returns a Status Code which indicates the state of the device or the reason for failure of a requested operation. 88RF PICCs are known to return misleading Status Codes under certain circumstances:

Write User Zone command

The Write User Zone command returns Status Code $A1 and NACK when L greater than $0F is sent. A Status Code $A3 is expected. The write operation fails and no data is written.

Write System Zone command

The Write System Zone command returns Status Code $B0 and ACK when the integrated checksum option is used in the encryption communication mode. A Status Code $00 is expected. The write operation succeeds and the data is written to the EEPROM correctly.

The Write System Zone command returns Status Code $C9 and NACK when PARAM = $02 is sent. A Status Code $A1 is expected. The write operation fails and no data is written.

The Write System Zone command returns Status Code $00 and NACK when PARAM = $0C and an invalid ADDR is sent. A Status Code $A2 is expected. The operation fails and no data is written.

Customers are advised that past and future products may return Status Codes that are different. The ACK/NACK byte reports if a requested operation has passed or failed; the Status code contains additional information.

T.5 Encryption Activation Change [88RF]

One byte value in the Encryption Activation procedure has been changed to allow 88RF PICCs to be used with the AT88SC018 CryptoMemory Companion chip. This change may impact customers migrating from 88SC PICCs to 88RF PICCs if the Encryption Communication Security mode is used.

When the host calculates the Authentication Activation Challenge at Step 8. in Appendix K.8, a value of $FF must be substituted in the calculation (in place of the actual 88RF PICC AAC value of $55).

This change is intentional.

Appendix U Revision History

Doc. Rev.	Date	Comments
5276F	01/2014	Add MVA1 ordering option. Remove MR1 ordering option for 16Kb and 32Kb devices. Update footers and disclaimer page.
5276E	10/2012	Decrease absolute maximum operating temperature (Junction) from (-40° to 85°C) to (-25°C to 85°C). Decrease industrial temperature range from (-40°C to 85°C) to (25°C to 85°C) for AT88SC0808CRF, AT88SC1616CRF, AT88SC3216CRF, and AT88SC6416CRF.
5276D	08/2012	Remove MY1 package option. Update template and Atmel logo.
5276C	03/2009	Remove AT88SC0104CRF, AT88SC0204CRF, AT88SC0404CRF. Add AT88RF04C Specifications.
5276B	03/2009	Add all CryptoRF Security Function Specifications. This Specification now requires an LLA license. Removed LLA August 2009.
5276A	07/2008	Initial document summary release.

Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**

© 2014 Atmel Corporation. / Rev.: Atmel-5276G-CryptoRF-AT88SC0808CRF-1616CRF-3216CRF-6416CRF-AT88RF04C-Datasheet_012014.

Atmel®, Atmel logo and combinations thereof, CryptoMemory®, CryptoRF®, and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.

DISCLAIMER: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death (“Safety-Critical Applications”) without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.