ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

MAX66240

DeepCover Secure Authenticator with ISO 15693, SHA-256, and 4Kb User EEPROM

General Description

DeepCover® embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The DeepCover Secure Authenticator (MAX66240) is a transponder IC that combines an ISO/IEC 15693 and ISO 18000-3 Mode 1-compatible RF front-end, a FIPS 180-based SHA-256 engine, and 4096 bits of user EEPROM in a single chip. A bidirectional security model enforces two-way authentication between a host system and the MAX66240. Each device has its own guaranteed unique 64-bit ROM ID that is factory programmed into the chip. This ROM ID is used as a fundamental input parameter for cryptographic operations and serves as an electronic serial number within the application.

Features and Benefits

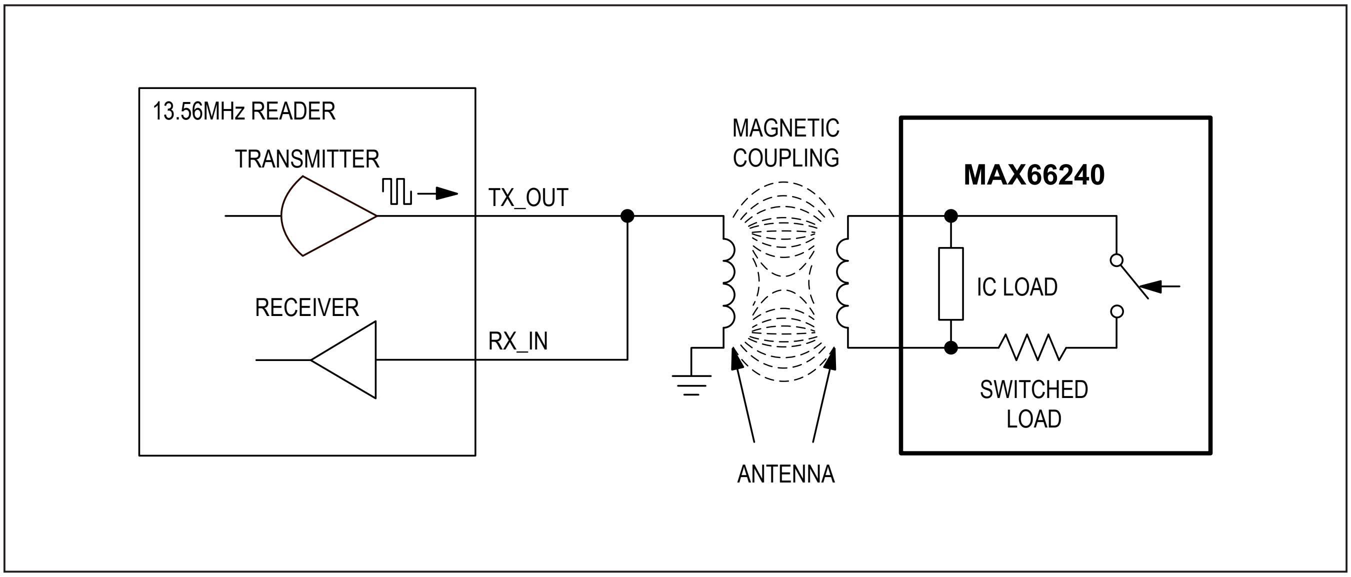
- Dedicated Hardware-Accelerated SHA Engine for Generating SHA-256 MACs
- Strong Authentication with a High Bit Count User-Programmable Secret and Input Challenge
- 4096 Bits of User EEPROM with User-Programmable R/W Protection Options Including OTP/EPROM Emulation Mode
- Unique Factory-Programmed 64-Bit Identification Number
- ISO/IEC 15693: Up to 26kbps
- ±2kV HBM ESD Protection for All Pins

Applications

- Access Control
- Asset Tracking
- Printer Cartridge Configuration and Monitoring
- Medical Sensor Authentication and Calibration
- System Intellectual Property Protection

***Ordering Information* appears at end of data sheet.**

Typical Application Circuit



DeepCover is a registered trademark of Maxim Integrated Products, Inc.

For related parts and recommended products to use with this part, refer to www.maximintegrated.com/MAX66240.related.

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND........-0.5V to +4.0V
Maximum RMS Current, AC1 to AC2................................30mA
Maximum Incident Magnetic Field Strength
(ISO/IEC 7810-compliant antenna) 141.6dBµA/m
Operating Temperature Range.......................... -40°C to +85°C
Junction Temperature..+150°C
Storage Temperature Range........................... -55°C to +125°C
Lead Temperature (soldering, 10s) ....+300°C
Soldering Temperature (reflow).......................................+260°C

Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Package Thermal Characteristics (Note 1)

SO
Junction-to-Ambient Thermal Resistance (θ_{JA}).........136°C/W
Junction-to-Case Thermal Resistance (θ_{JC})..............38°C/W

TDFN
Junction-to-Ambient Thermal Resistance (θ_{JA})...........60°C/W
Junction-to-Case Thermal Resistance (θ_{JC})..............30°C/W

Note 1: Package thermal resistances were obtained using the method described in JEDEC specification JESD51-7, using a four-layer board. For detailed information on package thermal considerations, refer to **www.maximintegrated.com/thermal-tutorial**.

Electrical Characteristics

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SHA-256 ENGINE						
Computation Time	t_{CSHA}	(Note 3)			2	ms
EEPROM						
Programming Time for a 32-Bit Page Block or Protection	t_{PROG}	(Note 4)			10	ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 5, 6)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Notes 7, 8, 9)	10			Years
RF PORT						
Carrier Frequency	f_C	(Note 10)	13.553	13.560	13.567	MHz
Internal Tuning Cap	C_{TUN}	f = 13.56MHz (Note 11)		27.5		pF
Operating Field	H_{ISO}	(Note 10)	150		5000	mA/m
Activation Field Strength	H_{MIN_10}	T_A = +25°C, 10% modulation (Notes 11, 12)		94		dBµA/m
	H_{MIN_30}	T_A = +25°C, 30% modulation (Notes 11, 12)		104		
	H_{MIN_100}	T_A = +25°C, 100% modulation (Notes 11, 12)		103.5		
Write/SHA Field Strength	H_{WR}	T_A = +25°C (Notes 11, 12, 13)		113		dBµA/m
RF Access in Progress Time	t_{RFAIP}			1.1		ms
10% Carrier Modulation Index MI = (A - B)/(A + B)	CMI_10	(Notes 10, 11)	10		30	%
100% Carrier Modulation Index MI = (A - B)/(A + B)	CMI_100	(Notes 10, 11)	95		100	%
10% Modulation Min Pulse Width	$t_{1\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Notes 11, 14)		7.0		µs

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
10% Modulation Max Pulse Width	t_1 MAX	Refer to ISO 15693-2 Section 7.1 (Note 11)			9.44	µs
10% Modulation Min Low Time	t_2 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 11, 14)		7.0		µs
10% Modulation Max Low Time	t_2 MAX	Refer to ISO 15693-2 Section 7.1 (Note 11)			9.44	µs
10% Modulation Min Rise Time	t_3 MIN	Refer to ISO 15693-2 Section 7.1 (Note 11)	0			µs
10% Modulation Max Rise Time	t_3 MAX	Refer to ISO 15693-2 Section 7.1 (Notes 11, 14)		2.5		µs
100% Modulation Min Pulse Width	t_1 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 11, 15)		6.5		µs
100% Modulation Min Pulse Width	t_1 MAX	Refer to ISO 15693-2 Section 7.1 (Note 11)			9.44	µs
100% Modulation Max Pulse Width	t_2 MIN	Refer to ISO 15693-2 Section 7.1 (Notes 11, 15)		6.5		µs
100% Modulation Max Low Time	t_2 MAX	Refer to ISO 15693-2 Section 7.1 (Note 11)			9.44	µs
100% Modulation Min Rise Time	t_3 MIN	Refer to ISO 15693-2 Section 7.1 (Note 11)	0			µs
100% Modulation Max Rise Time	t_3 MAX	Refer to ISO 15693-2 Section 7.1 (Notes 11, 15)		3.0		µs

Note 2: Limits are 100% production tested at T_A = +25°C or T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are at +25°C.

Note 3: For commands where the t_{CSHA} interval occurs see the applicable communication examples sections. For RF commands, the interval begins after the EOF of a valid request frame. The interval ends once the device's self-timed SHA-256 computation cycle is complete.

Note 4: For commands where the t_{PROG} interval occurs see the applicable communication examples sections. For RF commands, the interval begins after the EOF of a valid request frame. The interval ends once the device's self-timed EEPROM write cycle is complete.

Note 5: Write-cycle endurance is tested in compliance with JESD47G.

Note 6: Not 100% production tested; guaranteed by reliability qualification.

Note 7: Data retention is tested in compliance with JESD47G.

Note 8: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to the data sheet limit at operating temperature range is established by reliability testing.

Note 9: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended.

Note 10: System requirement.

Note 11: Guaranteed by design and/or characterization only. Not production tested.

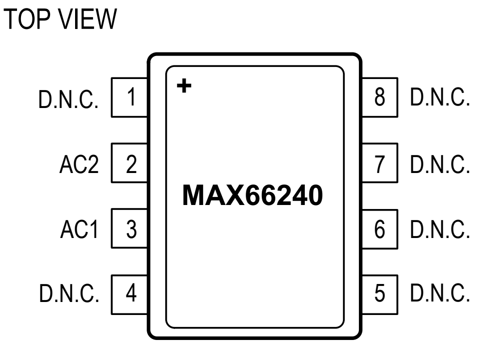
Note 12: Characterized in accordance with ISO/IEC 10373-7.

Note 13: Applies to Read/Write Scratchpad (writing), Write Memory, Compute and Read Page MAC, Set Protection, Authenticated Write Memory RF Setup, Authenticated Write Memory RF Execute, Authenticated Set Protection RF Setup, and Authenticated Set Protection RF Execute commands.

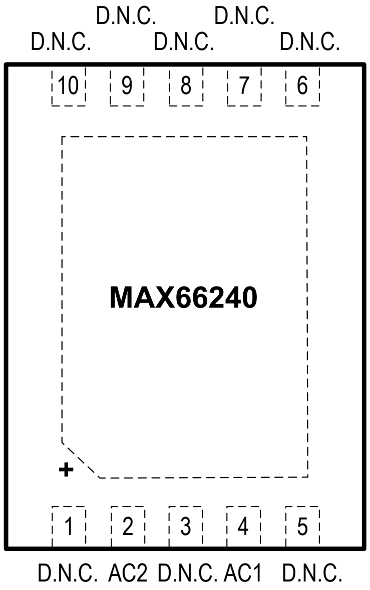
Note 14: Field strength between 350mA/m and 3A/m.

Note 15: Field strength between 350mA/m and 5A/m.

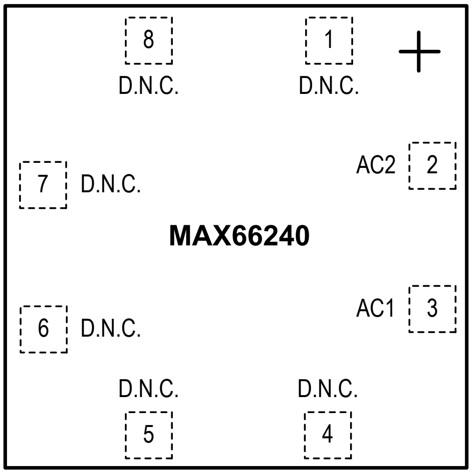
Pin Configurations



SO



TDFN



BUMPED DIE

Pin Descriptions

PIN		NAME	FUNCTION
SO/ BUMPED DIE	TDFN		
1, 4–8	1, 3, 5–10	D.N.C.	Do Not Connect
2	2	AC2	Antenna Connection
3	4	AC1	Antenna Connection

Detailed Description

The MAX66240 transponder combines an ISO 15693 RF front-end, a SHA-256 engine, 4096 bits of user EEPROM organized as 16 256-bit pages, protection control, status memory, and a 64-bit ROM ID in a single chip. A 256-bit scratchpad assists when installing a new secret or stores the challenge when computing a page MAC.

It is common for a secure authentication IC to be attacked using a variety of sophisticated die-level methods to extract secure data, reverse device settings, etc., in an effort to compromise a system security implementation. To provide the highest affordable protection against this inevitable malicious attack, the MAX66240 employs proprietary die-level physical techniques, circuits, and crypto methods to protect sensitive data, control signals, and control settings.

There are multiple programmable options for the 4Kb user array including unrestricted read/write and four protection modes: read protection, write protection, EPROM emulation mode, and authentication protection. Read protection prevents user read-access to the memory, which effectively extends the secret into the protected memory. The data remains accessible only for the SHA-256 engine. Write protection prevents changes to the memory data. EPROM emulation mode logically ANDs memory data with incoming new data, which allows changing bits from 1 to 0, but not vice versa. By changing one bit at a time, this mode could be used to create a nonvolatile, nonresettable counter. EPROM emulation mode requires that the memory is not write protected. Authentication protection, if activated, requires that the host prove itself as authentic (i.e., knows the MAX66240 secret) to modify the memory by supplying a correct MAC that is based on the device secret, its ROM ID, memory data, and the new data to be copied to EEPROM. If the authentication hurdle is passed, the write protection and EPROM emulation mode protections still determine the effect of the write access. Any protection, if activated, applies to individual memory pages. As a factory default, none of the protections is activated. Once authentication protection is activated, the reader must authenticate itself for memory writes as well as for additional changes to the memory protection.

In addition to its important use as a unique data value in cryptographic SHA-256 computations, the device's 64-bit ROM ID can be used to electronically identify the object to which the MAX66240 is associated. Applications of the MAX66240 include, access control, asset tracking, printer cartridge configuration and monitoring, medical sensor authentication and calibration, and system intellectual property protection.

Overview

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the MAX66240. The device has six main data components: 16 256-bit pages of user EEPROM, a 256-bit secret, protection control/status memory, 512-bit SHA-256 engine, 64-bit ROM ID, and a 256-bit scratchpad.

Figure 2 shows the applicable commands and the affected data fields. The network function commands allow the reader to identify all transponders in its range and to change their state, e.g., to select one for further communication. The protocol required for these network function commands is described in the *Network Function Commands* section. The memory and control functions fall into five categories: ISO 15693 generic commands, secret installation, memory access, protection setting, and MAC computation. The protocol for these commands is described in the *Memory and Control Function Commands* section. All data is read and written least significant bit (LSb) first, starting with the least significant byte (LSB).

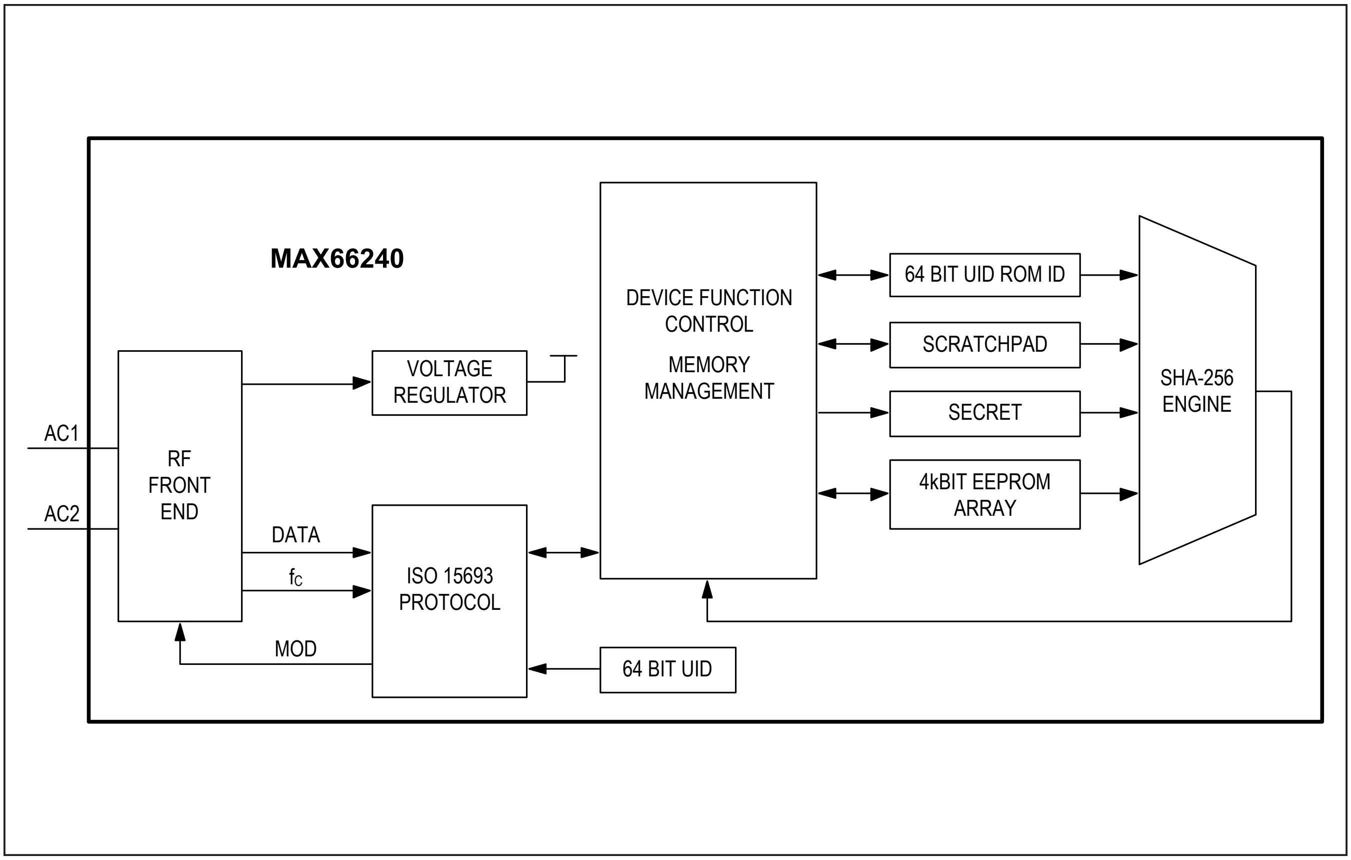


Figure 1. Block Diagram

COMMAND TYPE:	AVAILABLE COMMANDS:	DATA FIELD AFFECTED:
NETWORK FUNCTION COMMANDS	INVENTORY	UID, AFI, DSFID
	STAY QUIET	UID
	SELECT	UID
	RESET TO READY	(N/A)
MEMORY AND CONTROL FUNCTION COMMANDS	GET SYSTEM INFORMATION	UID, AFI, DSFID, CONSTANTS
	WRITE MEMORY	MFGCODE, USER MEMORY, PROTECTION SETTINGS
	READ MEMORY	MFGCODE, USER MEMORY, PROTECTION SETTINGS
	READ SINGLE BLOCK	SELECTED MEMORY BLOCK, PROTECTION SETTINGS
	READ MULTIPLE BLOCKS	SELECTED MEMORY BLOCKS, PROTECTION SETTINGS
	SET PROTECTION	MFGCODE, PROTECTION SETTINGS
	READ STATUS	MFGCODE, PROTECTION SETTINGS, PERSONALITY BYTES
	READ/WRITE SCRATCHPAD	MFGCODE, SCRATCHPAD
	LOAD AND LOCK SECRET	MFGCODE, SECRET AND LOCK STATUS, SCRATCHPAD
	COMPUTE AND LOCK SECRET	MFGCODE, SECRET AND LOCK STATUS, USER MEMORY, SCRATCHPAD, PROTECTION SETTING
	COMPUTE AND READ PAGE MAC	MFGCODE, SECRET, ROM ID, USER MEMORY, SCRATCHPAD
	AUTHENTICATED WRITE MEMORY RF SETUP	MFGCODE, USER MEMORY, PAGE BLOCK NUMBER, SECRET, PROTECTION SETTINGS
	AUTHENTICATED WRITE MEMORY RF EXECUTE	MFGCODE, USER MEMORY
	AUTHENTICATED SET PROTECTION RF SETUP	MFGCODE, MEMORY PAGE NUMBER, SECRET, PROTECTION SETTINGS
	AUTHENTICATED SET PROTECTION RF EXECUTE	MFGCODE, PROTECTION SETTINGS
	GET 1-WIRE ROM ID	MFGCODE, ROM ID
	WRITE AFI	AFI BYTE
	LOCK AFI	AFI LOCK STATUS
	WRITE DSFID	DSFID BYTE
	LOCK DSFID	DSFID LOCK STATUS

Figure 2. Commands Overview

Parasite Power

The MAX66240 receives all energy necessary for its operation from the surrounding RF field, which needs to have a minimum strength as specified in the *Electrical Characteristics* table.

Unique Identification Number (UID)

Each MAX66240 contains a factory-programmed and locked identification number that is 64 bits long (Figure 3). The lower 28 bits are the serial number of the chip. The upper 36 bits are fixed at E02B00800h. The code in bit locations 49 to 56 identifies the chip manufacturer, according to ISO/IEC 7816-6/AM1. This code is 2Bh for Maxim. The UID is read accessible through the Inventory and Get System Information commands.

ROM ID

The read-only ROM ID is similar to the UID (Figure 4). The first 8 bits are a family code, which is E0h. The next 28 bits are a unique serial number. The next 20 bits are fixed at 2B000h. The last 8 bits are a cyclic redundancy check (CRC) of the first 56 bits. The CRC is generated using the polynomial $X^8 + X^5 + X^4 + 1$ (Figure 5). Additional information about this CRC is available in Application Note 27: *Understanding and Using Cyclic Redundancy Checks with Maxim iButton® Products*. The ROM ID is part of the input data to the SHA-256 engine. It is read accessible through the command Get 1-Wire ROM ID.

MSb LSb

64 57	56 49	48 45	44 37	36 29	28 1
E0h	2Bh	0h	04h	00h	Serial Number

Figure 3. 64-Bit UID

MSb LSb

8-bit CRC Code	2Bh	0h	00h	28-bit Serial Number	8-bit Family Code (E0h)
MSb LSb				MSb LSb	MSb LSb

Figure 4. 64-Bit ROM ID

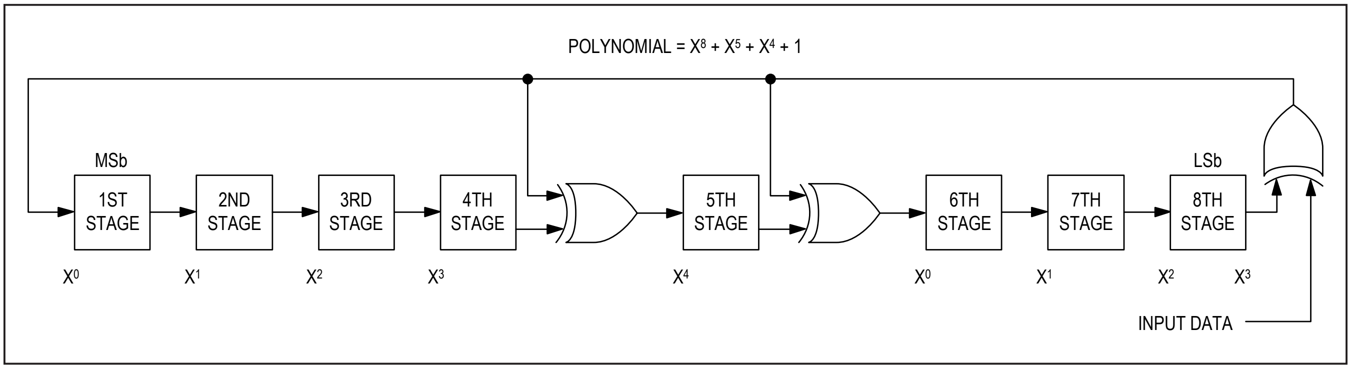


Figure 5. 8-Bit CRC for the ROM ID

iButton is a registered trademark of Maxim Integrated Products, Inc.

Memory Resources

The memory of the MAX66240 consists of user EEPROM, secret memory, an SRAM scratchpad, personality registers, ROM ID, and two ISO 15693-specific bytes. Table 1 shows the size, access mode, and purpose of the various memory areas. Brackets around an access mode indicate possible restrictions, such as write protection or read protection.

The user memory is organized as 16 pages of 32 bytes each (Figure 6). A page is divided into 8 page blocks of 32 bits each. With the MAX66240, the page protection applies to individual memory pages. The user memory is written in page blocks. If not read protected, the memory can be read starting at any page block of any page. The protocol allows reading multiple page blocks and pages up to the end of the memory in a single read command flow.

The secret is either directly written (loaded) or computed. This write access always encompasses the entire 32-byte secret. To protect against transmission errors, the new secret (loading) or a partial secret (computing) is first written to the scratchpad from where it can be read for verification. As the name implies, the secret memory is not user readable. To protect a secret from changes, it must be write protected (locked).

Page protection control is activated through the Write Page Protection command. Besides write protection, read protection and EPROM emulation mode, the MAX66240 supports authentication protection. If authentication protection is activated, changes to the page protection settings as well as writing to the protected user memory require that the reader provide a valid MAC for the operation. Once a protection is activated, it cannot be reversed. The protection settings as well as the personality registers are read accessible through the Read Status command. See the *Memory and Control Function Commands* section for command flow details.

Depending on the command, the ROM ID may be required in the MAC computations. This makes the MAC generated by a MAX66240 or written to the MAX66240 (if authentication protection is activated) device-specific, even if the values of all other data elements are identical. Instead of requiring the reader to derive the ROM ID from the UID, the MAX66240 supports a special command to read the ROM ID directly.

Note that the ISO 15693 standard commands Read Single Block and Read Multiple Blocks do not address the user memory by page number and page block number. Instead, they use absolute block numbers counting from 0 to 127. Figure 7 shows how these absolute numbers map to the user memory.

Table 1. Memory Resources

NAME	SIZE (BYTES)	ACCESS MODE	PURPOSE
User Memory (EEPROM)	512	(Read), (Write), Internal Read	Application-specific data storage; also used for MAC computations.
Secret Memory (EEPROM)	32	(Write), (Compute), Internal Read	Storage of the secret that is used for MAC computations.
Scratchpad (SRAM)	32	Read, Write, Internal Read	Intermediate data storage when installing a secret; also used to store the challenge for a MAC computation.
Personality Registers	4	Read, Internal Read	Lock status indicator for the secret and read access to the device's manufacturer ID (factory preprogrammed parts).
ROM ID	8	Read, Internal Read	Used for MAC computations.
Application Family Identifier (AFI)	1	Read, (Write)	Can be used during the inventory phase to narrow the number of transponders that participate in the discovery or anti-collision process.
Data Storage Format Identifier (DSFID)	1	Read, (Write)	User byte that can provide details on how the data in the user memory is structured.

	PG. BLOCK 7				PG. BLOCK 6				PG. BLOCK 5				PG. BLOCK 4				PG. BLOCK 3				PG. BLOCK 2				PG. BLOCK 1				PG. BLOCK 0			
	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0	B3	B2	B1	B0
Page 0																																
Page 1																																
Page 2																																
Page 3																																
Page 4																																
Page 5																																
Page 6																																
Page 7																																
Page 8																																
Page 9																																
Page 10																																
Page 11																																
Page 12																																
Page 13																																
Page 14																																
Page 15																																

Figure 6. User Memory Map

	PG. BLOCK 7	PG. BLOCK 6	PG. BLOCK 5	PG. BLOCK 4	PG. BLOCK 3	PG. BLOCK 2	PG. BLOCK 1	PG. BLOCK 0
Page 0	Block 7	Block 6	Block 5	Block 4	Block 3	Block 2	Block 1	Block 0
Page 1	Block 15	Block 14	Block 13	Block 12	Block 11	Block 10	Block 9	Block 8
Page 2	Block 23	Block 22	Block 21	Block 20	Block 19	Block 18	Block 17	Block 16
Page 3	Block 31	Block 30	Block 29	Block 28	Block 27	Block 26	Block 25	Block 24
Page 4	Block 39	Block 38	Block 37	Block 36	Block 35	Block 34	Block 33	Block 32
Page 5	Block 47	Block 46	Block 45	Block 44	Block 43	Block 42	Block 41	Block 40
Page 6	Block 55	Block 54	Block 53	Block 52	Block 51	Block 50	Block 49	Block 48
Page 7	Block 63	Block 62	Block 61	Block 60	Block 59	Block 58	Block 57	Block 56
Page 8	Block 71	Block 70	Block 69	Block 68	Block 67	Block 66	Block 65	Block 64
Page 9	Block 79	Block 78	Block 77	Block 76	Block 75	Block 74	Block 73	Block 72
Page 10	Block 87	Block 86	Block 85	Block 84	Block 83	Block 82	Block 81	Block 80
Page 11	Block 95	Block 94	Block 93	Block 92	Block 91	Block 90	Block 89	Block 88
Page 12	Block 103	Block 102	Block 101	Block 100	Block 99	Block 98	Block 97	Block 96
Page 13	Block 111	Block 110	Block 109	Block 108	Block 107	Block 106	Block 105	Block 104
Page 14	Block 119	Block 118	Block 117	Block 116	Block 115	Block 114	Block 113	Block 112
Page 15	Block 127	Block 126	Block 125	Block 124	Block 123	Block 122	Block 121	Block 120

Figure 7. User Memory Access Using Absolute Block Numbers

ISO/IEC 15693 Interface

The communication between an HF reader and MAX66240 (transponder) is a master-transponder type transaction, and is based on the exchange of data packets. The reader initiates every transaction; only one side (reader or transponder) transmits information at any time. Each data packet begins with a start-of-frame (SOF) pattern and ends with an end-of-frame (EOF) pattern. A data packet delimited by an SOF and an EOF is called a frame (Figure 8). The last 2 bytes of an ISO 15693 frame are an inverted 16-bit CRC of the preceding data generated according to the CRC-16-CCITT polynomial X16 + X12 + X5 + 1 (Figure 9). This CRC is transmitted with the LSB first. For more details on the CRC-16-CCITT, refer to ISO 15693-3, Annex C. Frame information is modulated on a 13.56MHz carrier. The subsequent paragraphs are a concise description of the required modulation, coding, and basic timing.

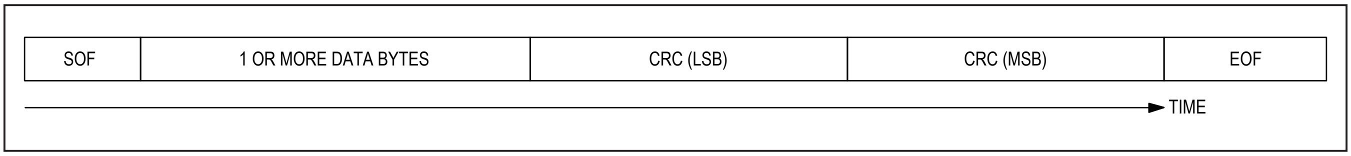


Figure 8. ISO/IEC 15693 Frame Format

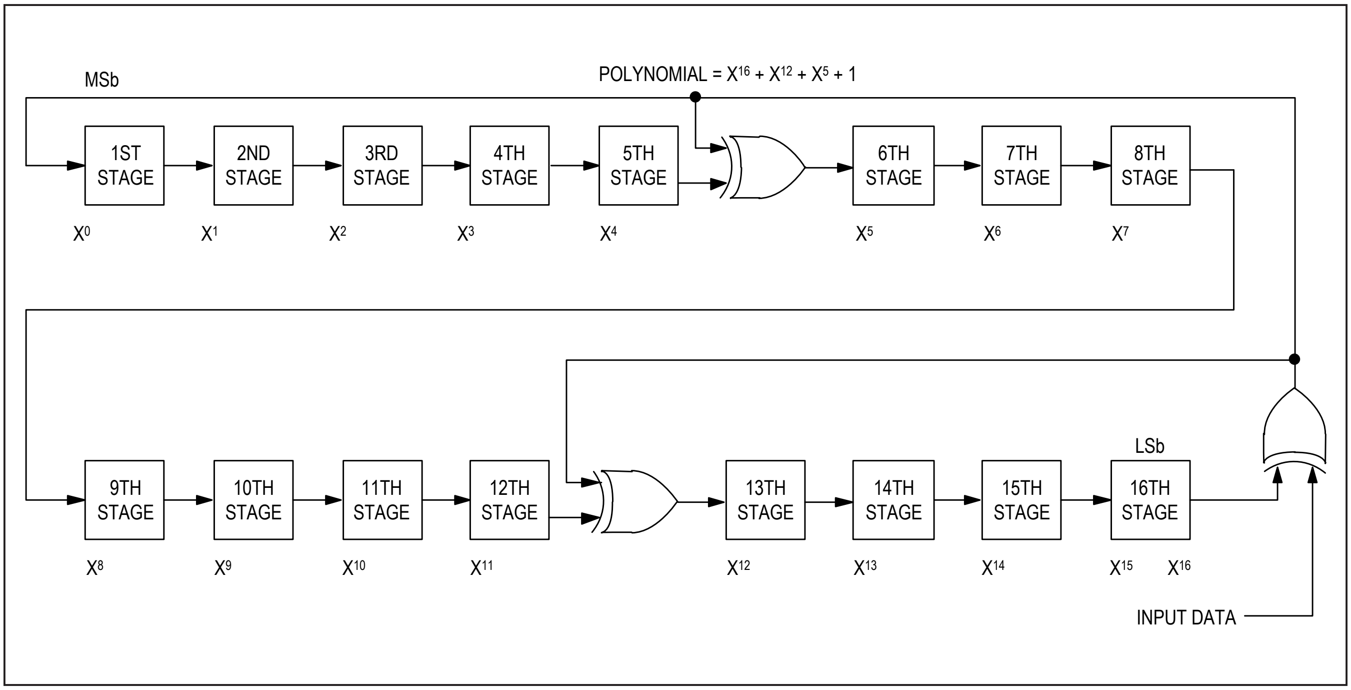


Figure 9. CRC-16-CCITT Generator

Reader to Transponder Communication

The communication from reader to transponder uses amplitude modulation (Figure 10); the modulation index can be either in the range of 10% to 30% or 100% (ISO 15693-2, Section 7.1). The standard defines two pulse-position data coding modes. The “1 out of 256” data coding mode transmits one 1 byte in 4.833ms, equivalent to a data rate of 1655bps (Figure 11). The location of a modulation pause during the 4.833ms conveys the value of the byte. The “1 out of 4” data coding mode transmits 2 bits in 75.52µs, equivalent to a data rate of 26,484bps (Figure 12). The location of a modulation pause during the 75.52µs conveys the value of the 2 bits. A byte is transmitted as a concatenation of four 2-bit transmissions, with the least significant 2 bits of the byte being transmitted first. The transmission of the SOF pattern also takes 75.52µs. The SOF pattern has two modulation pauses. The position of the second pause determines whether the frame uses the “1 out of 256” or “1 out of 4” data coding mode (Figure 13 and Figure 14, respectively). The transmission of the EOF pattern takes 37.76µs; the EOF is the same for both coding modes and has one modulation pause (Figure 15). For full details, refer to ISO 15693-2, Sections 7 and 8.

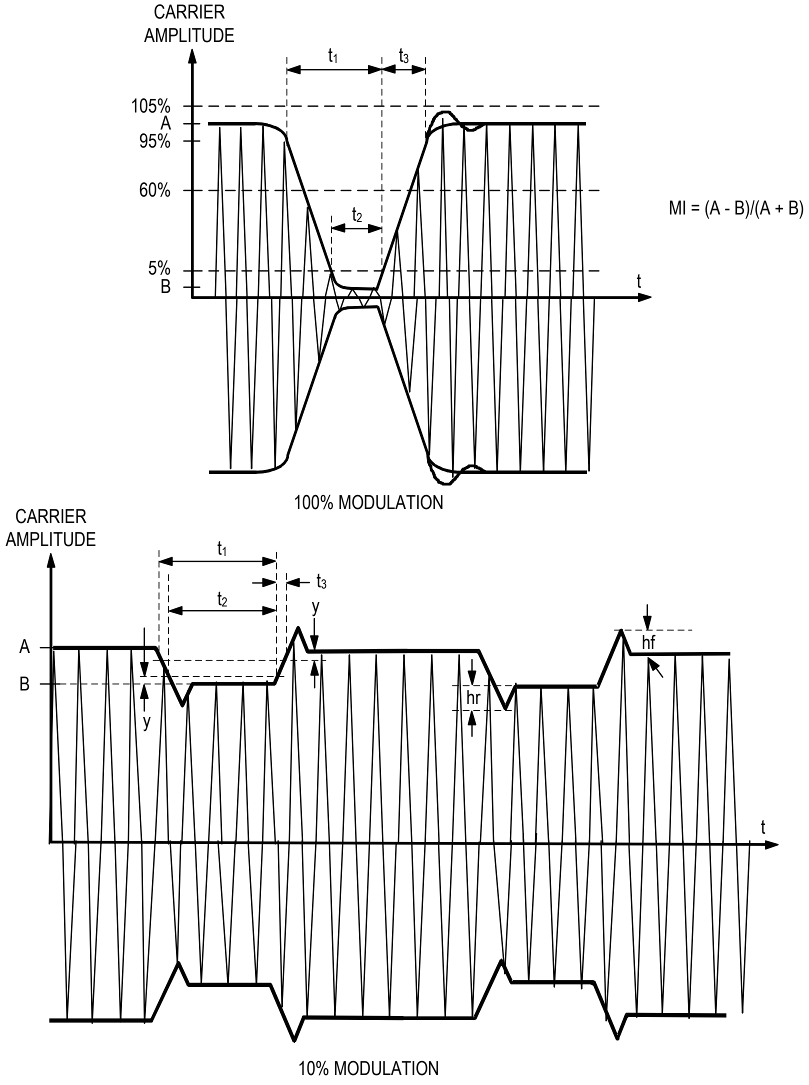


Figure 10. Reader to Transponder Modulation

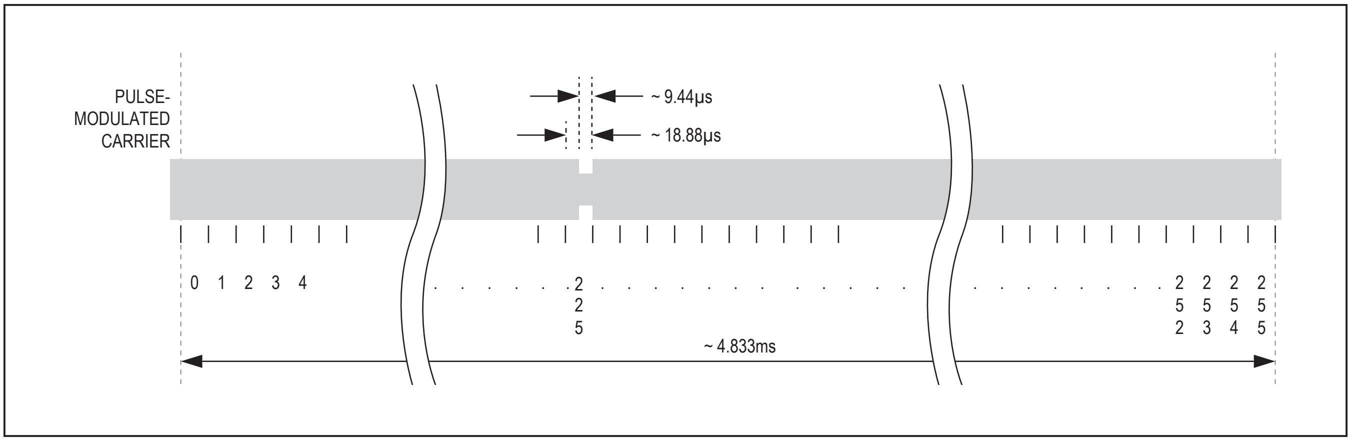


Figure 11. Reader to Transponder “1 Out of 256” Data Coding

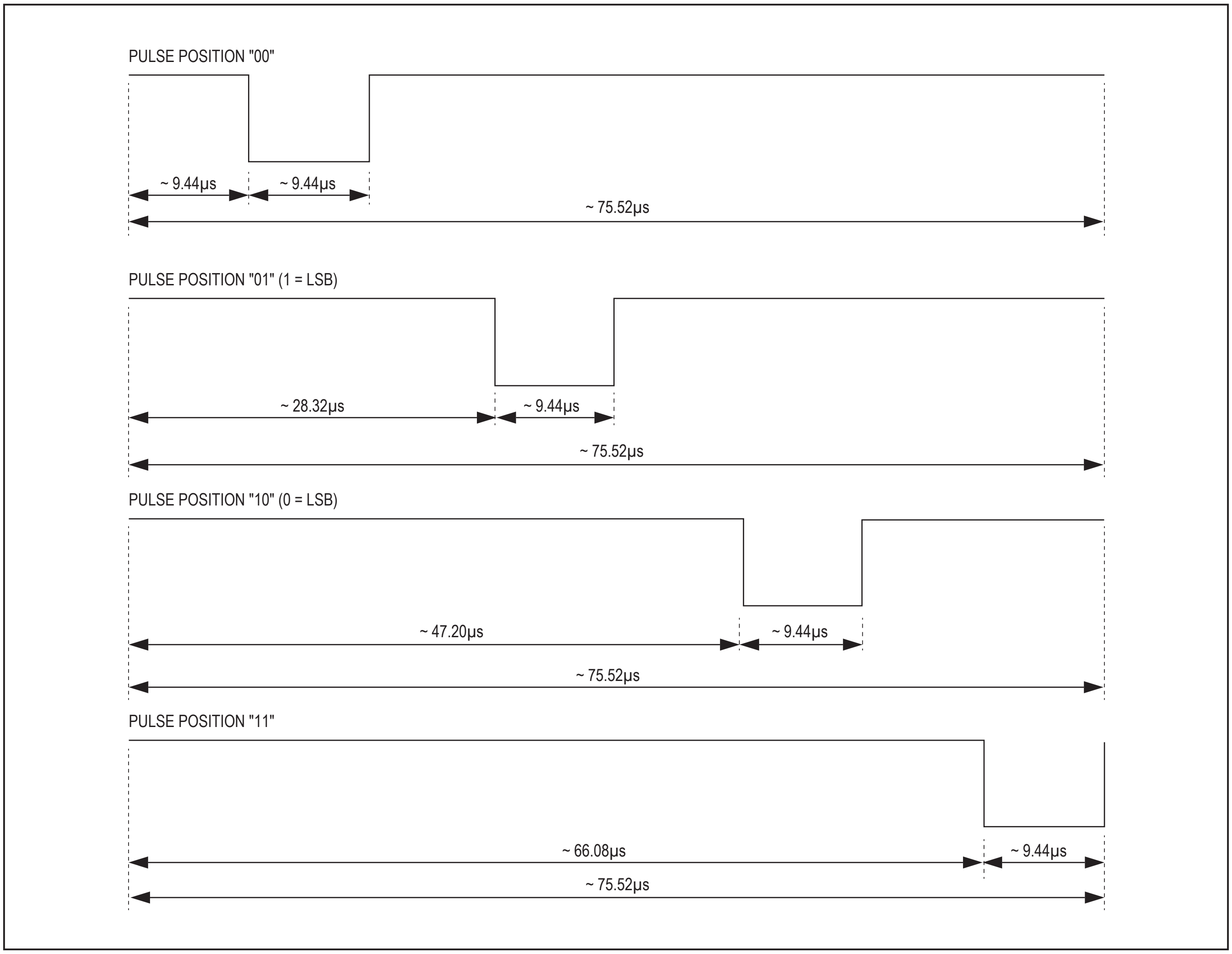


Figure 12. Reader to Transponder “1 Out of 4” Data Coding (Carrier Not Shown)

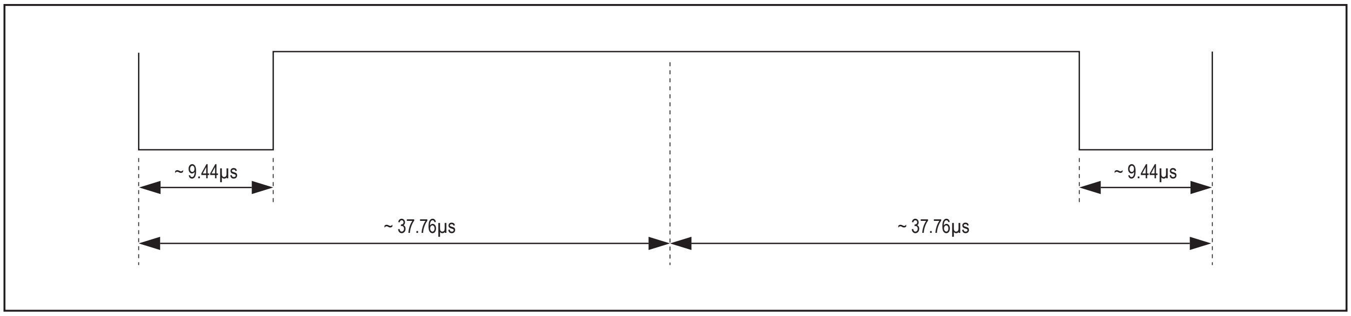


Figure 13. Reader to Transponder SOF for "1 Out of 256" Data Coding (Carrier Not Shown)

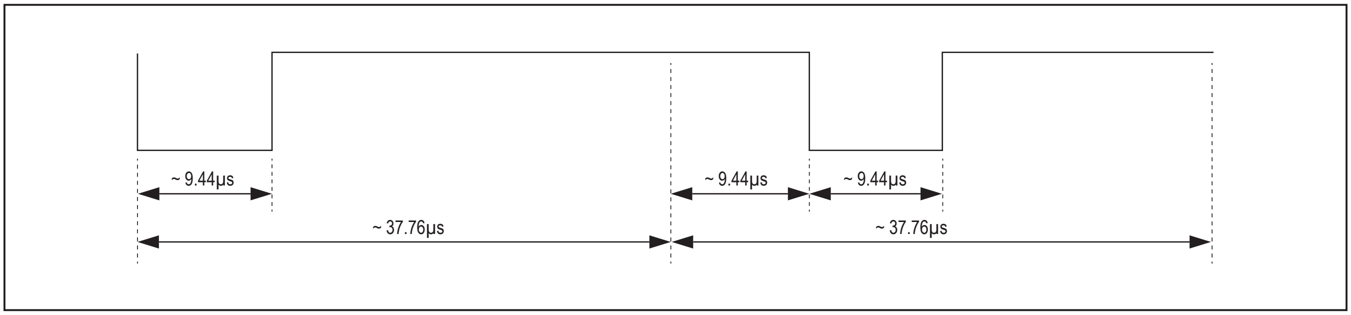


Figure 14. Reader to Transponder SOF for "1 Out of 4" Data Coding (Carrier Not Shown)

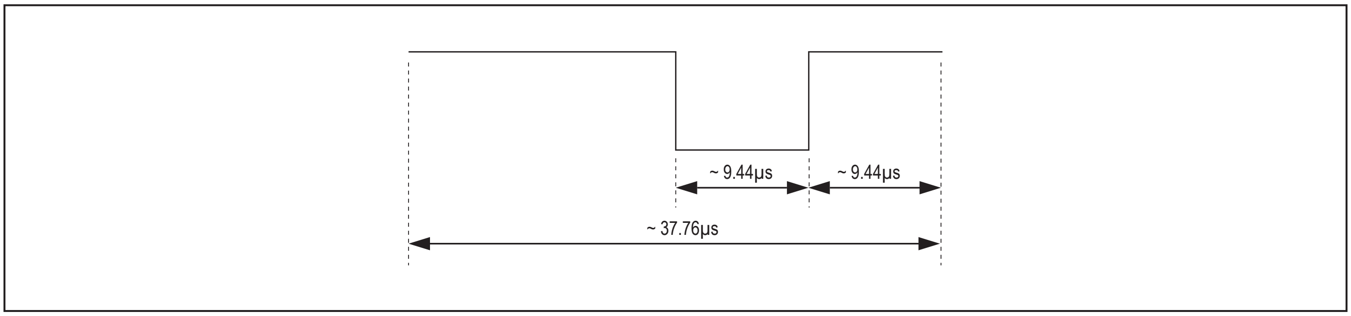


Figure 15. Reader to Transponder EOF (Identical for Both Coding Modes, Carrier Not Shown)

Transponder to Reader Communication

The Subcarrier_flag bit in the request data frame specifies the use of one or two subcarrier in the response frame. For the one subcarrier case, the subcarrier frequency is 423.75kHz. For the two subcarrier case, the subcarrier frequencies are 423.75kHz and 484.28kHz. The Data_rate_flag bit in the request data frame specifies the response frame data rate. Low data rate is approximately 6,600bps, and high data rate is approximately 26,500bps. The data rate varies slightly depending on the use of one or two subcarriers. The LSb is transmitted first.

In the single subcarrier high data rate case, one bit is transmitted in 37.76μs. For a logic 0, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. This is followed by 256 cycles of no modulation. For a logic 1, the transponder does not modulate for 256 cycles. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. An SOF or EOF is transmitted in approximately 151μs. For an SOF, the transponder does not modulate for 768 cycles. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. This is followed by a logic 1. For an EOF, the transponder sends a logic 0. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. This is followed by no modulation for 768 cycles. See Figure 16 and Figure 18 for more details. For low data rate, multiply all cycle counts and times by 4.

In the two subcarrier low data rate case, one bit is transmitted in 37.46μs. For a logic 0, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. Next, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 9 times. For a logic 1, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 9 times. Next, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 8 times. An SOF or EOF is transmitted in approximately 149.8μs. For an SOF, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 27 times. Next, the transponder modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. This is followed by a logic 1. For an EOF, the transponder sends a logic 0. It then modulates for 16 cycles then does not modulate for 16 cycles, which is repeated 24 times. Next, the transponder modulates for 14 cycles then does not modulate for 14 cycles, which is repeated 27 times. See Figure 17 and Figure 19 for more details. For low data rate, multiply all cycle counts and times by 4.

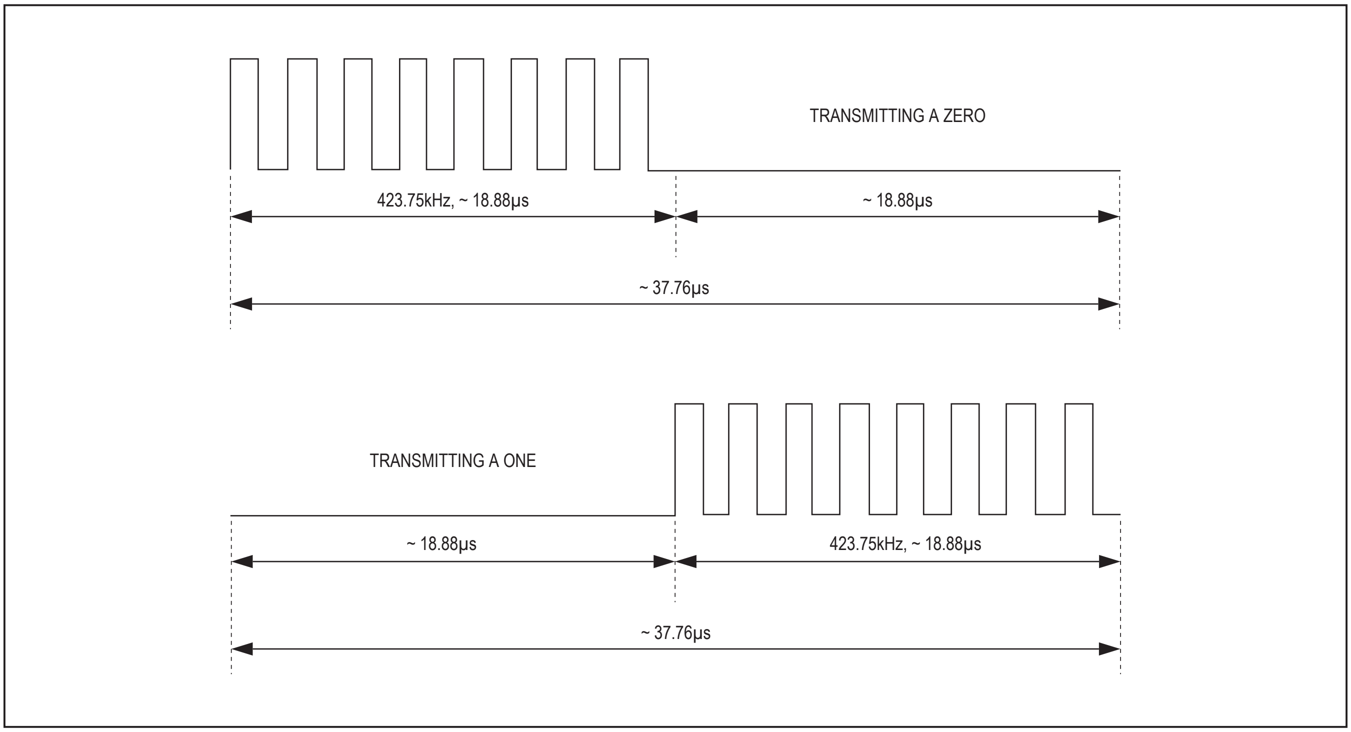


Figure 16. Transponder to Reader Coding, Single Subcarrier Bit Coding (High Data-Rate Timing)

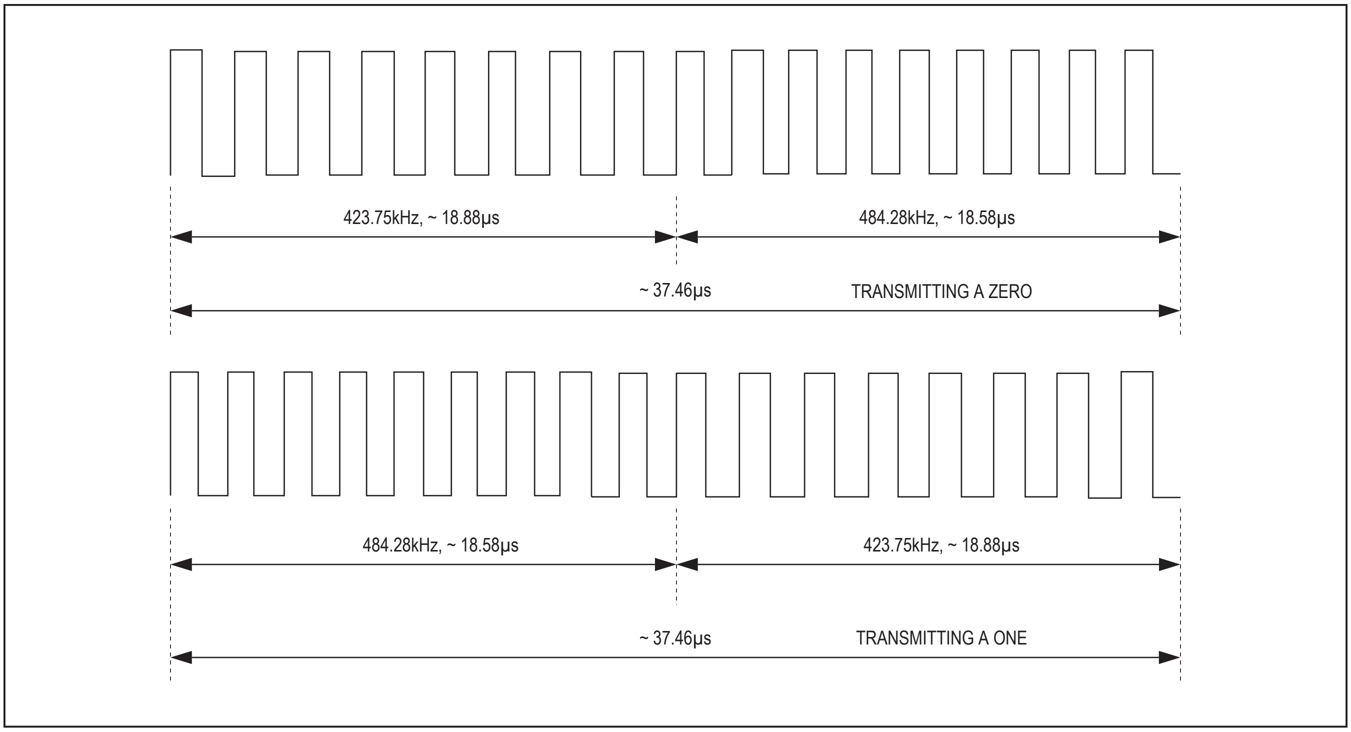


Figure 17. Transponder to Reader Coding, Two Subcarriers Bit Coding (High Data-Rate Timing)

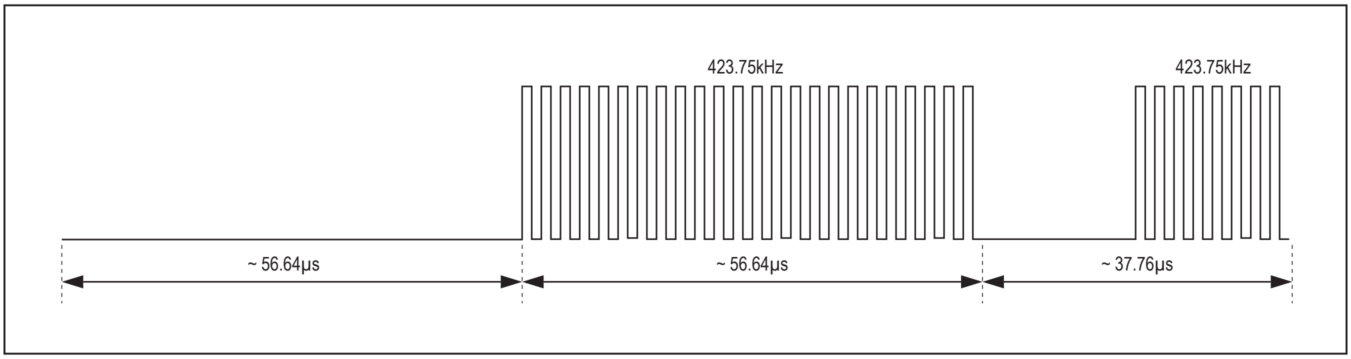


Figure 18. Transponder to Reader SOF, One Subcarrier (High Data Rate)

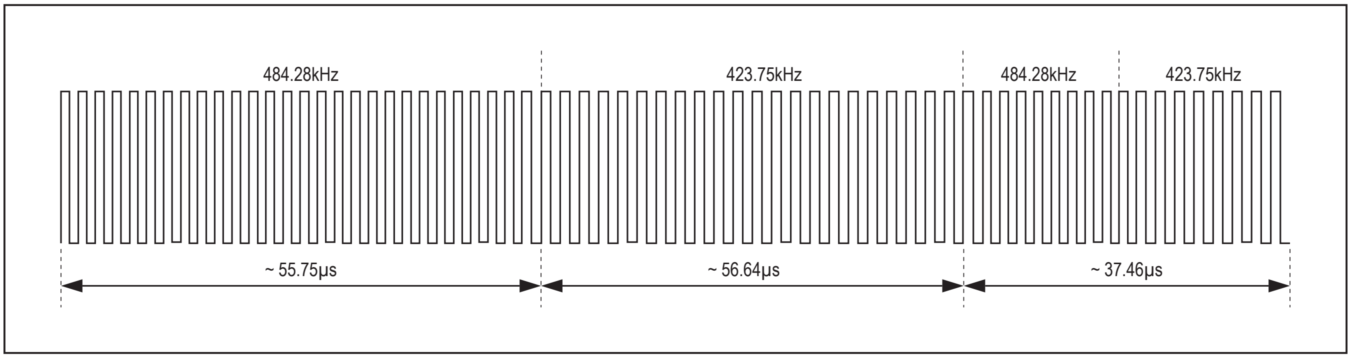


Figure 19. Transponder to Reader SOF, Two Subcarriers (High Data Rate)

ISO 15693 Transponder States and State Transitions

ISO 15693 defines four transponder states and three address modes. The states are power-off, ready, quiet, and selected. The address modes are nonaddressed, addressed, and select. The addressed mode requires that the reader include the transponder's UID in the request. Figure 20 shows how the Reset to Ready, Stay Quiet, and Select commands respond when changing the transponder's state. Table 2 shows how other commands respond depending on address mode and the transponder's state. Note that Stay Quiet never generates a response. For full details, refer to ISO 15693-2, Section 7.

Power-Off State

This state applies if the transponder is outside the reader's RF field. A transponder transitions to the power-off state when leaving the power-delivering RF field. When entering the RF field, the transponder automatically transitions to the ready state.

Ready State

In this state, a transponder has enough power to perform any of its functions. The purpose of the ready state is to have the transponder population ready to process the inventory command as well as other commands sent in the addressed or nonaddressed mode. A transponder can exit the ready state and transition to the quiet or the selected state upon receiving the Stay Quiet or Select command sent in addressed mode.

Quiet State

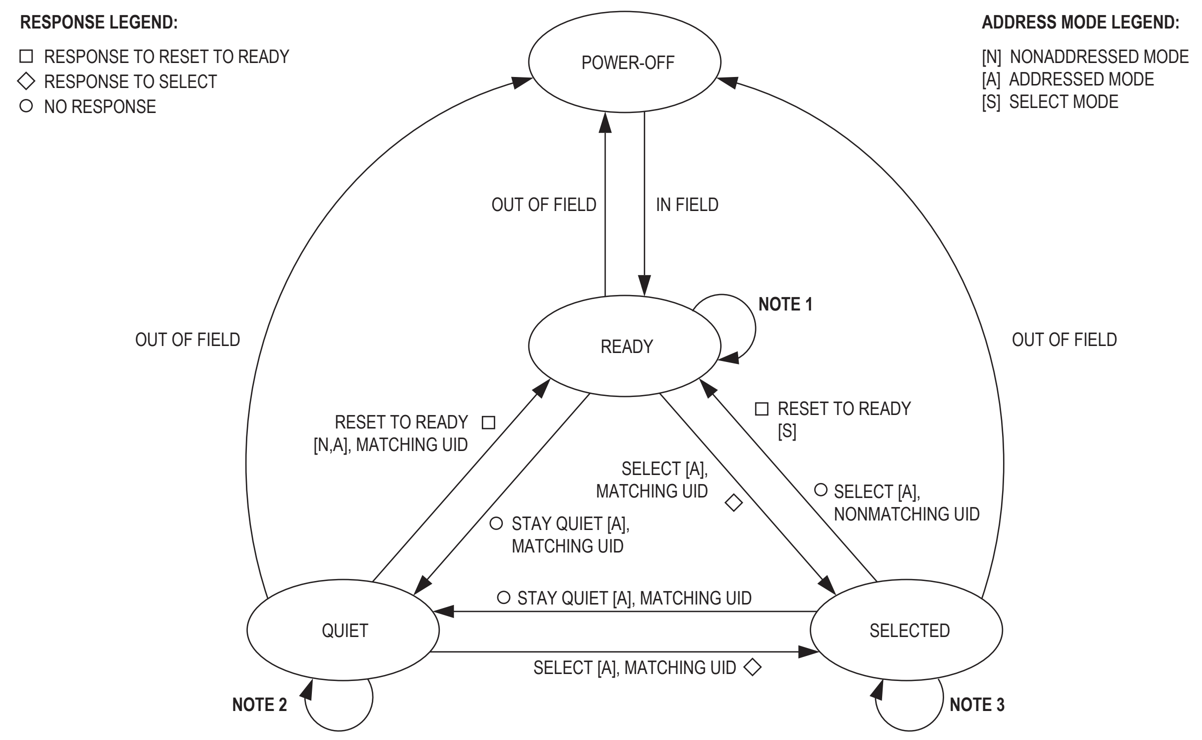
In this state, a transponder has enough power to perform any of its functions. The purpose of the quiet state is to silence transponders with which the reader does not want to communicate. Only commands sent with the addressed mode are processed. This way the reader can use the nonaddressed mode for communication with remaining transponders in the ready state. A transponder can exit the quiet state and transition to the ready state upon receiving the Reset to Ready command in addressed or nonaddressed mode. It can also transition to the selected state upon receiving Select commands sent in addressed mode.

Selected State

In this state, a transponder has enough power to perform any of its functions. The purpose of the selected state is to isolate the transponder with which the reader wants to communicate. Commands are processed regardless of the address mode in which they are sent, including the Inventory command. With multiple transponders in the RF field, the reader can put one transponder in the selected state, leaving all others in the ready state. For a transponder in the selected state, the reader can use the selected mode, which keeps the request data packets as short as with the nonaddressed mode. A new transponder entering the RF field will not disturb communication since it powers up in the ready state. A transponder can exit the selected state and transition to the ready state upon receiving the Reset to Ready command sent in nonaddressed or addressed mode. It can also transition to the quiet state upon receiving the Stay Quiet command sent in the addressed mode. A transponder also transitions from selected to ready upon receiving a Select command if the UID in the request is different from the transponder's own UID. In this case, the reader's intention is to transition another transponder with the matching UID to the selected state. If the transponder already in the selected state does not recognize the command, e.g., due to a bit error, two transponders could be in the selected state. To prevent this from happening, the reader should use the Reset to Ready or the Stay Quiet command to transition a transponder out of the selected state.

Table 2. Command Response vs. Transponder State and Address Mode Combinations

TRANSPONDER STATES	ADDRESS MODES		
	NONADDRESSED MODE (Address_flag = 0; Select_flag = 0)	ADDRESSED MODE (Address_flag = 1; Select_flag = 0)	SELECT MODE (Address_flag = 0; Select_flag = 1)
Power-Off	(Inactive)	(Inactive)	(Inactive)
Ready	Respond	Respond	Do not respond
Quiet	Do not respond	Respond	Do not respond
Selected	Respond	Respond	Respond



NOTE 1: THE TRANSPONDER PROCESSES THE INVENTORY COMMAND, AND PROCESSES OTHER COMMANDS IN NONADDRESSED MODE OR ADDRESSED MODE WITH MATCHING UID.

NOTE 2: THE TRANSPONDER DOES NOT PROCESS THE INVENTORY COMMAND, AND PROCESSES OTHER COMMANDS IN ADDRESSED MODE WITH MATCHING UID.

NOTE 3: THE TRANSPONDER PROCESSES THE INVENTORY COMMAND, AND PROCESSES OTHER COMMANDS IN NONADDRESSED MODE, ADDRESSED MODE WITH MATCHING UID, OR SELECT MODE.

Figure 20. ISO 15693 State Transition Diagram

Wait Times

ISO 15693 defines several standard wait times. For full details, refer to ISO 15693-2, Section 9.

The wait time from request frame EOF to response frame SOF is t_1. t_1 min is 318.6µs (4320 cycles), t_1 nom is 320.9µs (4352 cycles), and t_1 max is 323.3µs (4384 cycles). Commands that perform MAC calculations or write memory will extend t_1 by a command specific combination of t_{RFAIP}, t_{CSHA}, and t_{PROG}. If a 100% modulation pulse is detected during t_1, the transponder must restart its t_1 counter.

The 10% modulation ignore time after a request frame EOF is received is t_{MIT}. t_{MIT} min is 323.3µs (4384 cycles) + t_{NRT}, where t_{NRT} is the nominal response frame length.

The wait time between a response frame and a subsequent request frame is t_2. t_2 min is 309.2µs (4192 cycles).

The wait time between slot EOFs in an Inventory command where Nb_slots_flag is t_3. For 100% modulation, t_{3MIN} is 323.3µs (4384 cycles) + t_{SOF}, where t_{SOF} is the time requires to transmit a request frame SOF. For 10% modulation, t_3 min is 323.3µs (4384 cycles) + t_{NRT} + t_{2MIN}, where t_{NRT} is the nominal response frame length.

Network Function Commands

The ISO 15693 standard defines four network function commands: Inventory, Stay Quiet, Select, and Reset to Ready. Their purpose is to identify the UIDs of all transponders in the field (to Inventory) and to manage access to these transponders. Figure 20 shows how the network function commands are used to transition a transponder from one state to another.

Network Function Command Errors

Various error conditions can occur. If an error occurs, and the request is sent in addressed mode with matching UID or in select mode with the transponder in the Selected state, the transponder will transmit an error response. In any other mode/state combination, an error will result in no response. In case of an error response, the response begins with response flags of 01h, followed by a single-byte error code. Table 5 shows a matrix of commands, errors, and error codes.

Table 5. Network Function Command Error Code Matrix

ERROR EXPLANATION	Invalid Request Packet	Option Flag Set
ERROR CODE	02h	03h
FAILING COMMAND		
Reset to Ready	✓	✓
Select	✓	✓

Detailed Command Descriptions

Inventory

This command allows the reader to learn the UIDs and DSFIDs of all transponders in its RF field in an iterative process.

The AFI_flag determines if the AFI byte must be included in the request frame. The AFI byte is compared to the transponders AFI. The parameter byte determines the length of the mask. The LSb of the mask aligns with the LSb of the transponder's UID. The mask is compared to the transponder's UID. The Nb_slots_flag determines if a slot counter is concantenated with the mask for comparison to the transponder's UID. The slot counter starts at 0000b after the Inventory request frame is transmitted, and increments during the course of the Inventory command with every subsequent EOF sent by the reader. The AFI byte (if used) must match the transponder's AFI or be 00h, and the mask concatenated with the slot counter (if used) must match the transponder's UID for a response to be generated. This allows the reader to select transponders to respond to the Inventory command. The processing of an Inventory command ends if the transponder receives an SOF of a new request frame.

If a transponder meets all conditions to respond, it transmits a response frame. If multiple transponders meet the conditions, the response frames collide and may not be readable. The reader must eliminate the collision.

To identify all transponders in the RF field, the reader could begin with a mask length of 0 and activate the slot counter (Nb_slots_flag = 0). By using this method and going through all 16 slots, the reader has a chance to receive clean responses (i.e., the transponder is identified) as well as colliding responses. To prevent a transponder that has been identified from further participating in the collision management sequence, the reader transitions it to the quiet state. Next, the reader issues another Inventory command where the slot number that previously generated a collision is now used as a 4-bit mask, and runs again through all 16 slots. If a collision is found, another Inventory command is issued, this time with a mask that is extended at the higher bits by the slot counter value that produced the collision. This process is repeated until all transponders are identified. For a full description of the Inventory command processing by the transponder and the timing specifications, refer to ISO 15693 Part 3, Sections 8 to 9.

Inventory	
Command Code	01h
Parameter Byte	Mask Length (Table 6)
Conditions, Restrictions	The command is ignored unless the transponder is in the Ready or Selected state.
Protocol Variations	• Nb_slot_flag = 0, AFI_flag = 0, mask length = 0 • Nb_slot_flag = 0, AFI_flag = 0, mask length ≠ 0 • Nb_slot_flag = 0, AFI_flag = 1, mask length = 0 • Nb_slot_flag = 0, AFI_flag = 1, mask length ≠ 0 • Nb_slot_flag = 1, AFI_flag = 0, mask length = 0 • Nb_slot_flag = 1, AFI_flag = 0, mask length ≠ 0 • Nb_slot_flag = 1, AFI_flag = 1, mask length = 0 • Nb_slot_flag = 1, AFI_flag = 1, mask length ≠ 0
Other Notes	For the setting of the request flags (RQF), see Table 4. The mask pattern is transmitted only if the mask length is ≠ 0. The AFI is transmitted only if the AFI_flag bit in the request flags is set to 1.
Error Conditions (Error Response)	An error will result in no response.
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs

Table 6. Parameter Byte Bitmap

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

Bits [7:0]: Mask Length (MLEN). These bits specify the length of the mask. The mask (MASK) is transmitted only if MLEN is ≠ 0. The maximum mask length is 60 (3Ch, if Nb_slots_flag = 0) or 64 (40h, if Nb_slots_flag = 1).

Stay Quiet

This command addresses an individual transponder and transitions it to the Quiet state. The transponder does not send a response.

Stay Quiet	
Command Code	02h
Parameter Byte	N/A
Conditions, Restrictions	To transition to the Quiet state, the request must be sent in addressed mode with matching UID.
Protocol Variations	None
Other Notes	For the setting of the request flags (RQF), see Table 3.
Error Conditions (Error Response)	An error will result in no response.
t1 (Request Frame to Response Frame Delay)	None

Select

This command addresses an individual transponder and transitions it to the Selected state. The transponder transitioning to the Selected state sends a response. If there was a transponder with a different UID in the Selected state, then that transponder transitions to the Ready state without sending a response.

Select	
Command Code	25h
Parameter Byte	N/A
Conditions, Restrictions	To transition to the Selected state, the request must be sent in addressed mode with matching UID.
Protocol Variations	None
Other Notes	For the setting of the request flags (RQF), see Table 3.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6μs to 323.3μs

Reset to Ready

This command addresses an individual transponder and transitions it to the Ready state. The transponder transitioning to the Ready state sends a response.

Reset to Ready	
Command Code	26h
Parameter Byte	N/A
Conditions, Restrictions	To transition from the Quiet state to the Ready state, the request must be sent in nonaddressed mode or in addressed mode with matching UID. To transition from the Selected state to the Ready state, the request must be sent in select mode.
Protocol Variations	• If the transponder is in the Selected state, and the request is sent in addressed mode with nonmatching UID, the transponder transitions to the Ready state, but will not respond.
Other Notes	For the setting of the request flags (RQF), see Table 3.
Error Conditions (Error Response)	• Request data format error (response error code = 02h) • The Option_flag is set (response error code = 03h)
t1 (Request Frame to Response Frame Delay)	318.6µs to 323.3µs