ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

MAX66242

DeepCover Secure Authenticator with ISO 15693, I²C, 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 (MAX66242) is a transponder IC that combines an ISO/IEC 15693 and ISO 18000-3 Mode 1-compatible RF front-end, an I²C 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 MAX66242. 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.

In addition to the RF interface, the MAX66242 also has an I²C interface, which can operate as a slave or master port. When acting as a master, the MAX66242 can gather information from a connected sensor or peripheral device and relay its data via the RF port. When acting as a slave, the device can serve as an intermediary between a connected host and an RF reader. The MAX66242 can harvest energy from an active RF field. The configurable supply output can deliver up to 5mA given adequate field strength.

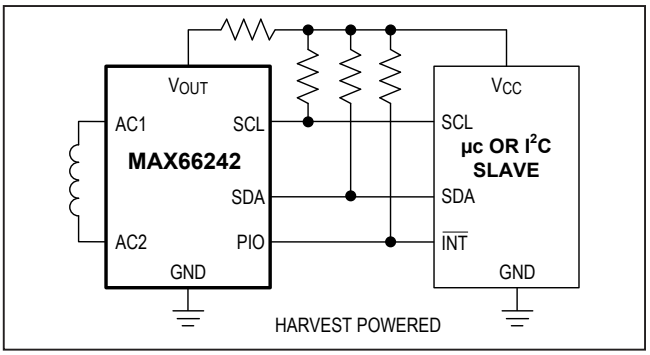
Applications

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

Benefits and Features

- Complete Counterfeit/Cloning/IP Protection Engine
  - SHA-256 Engine Runs a Symmetric Key-Based Bidirectional Secure Authentication
  - Strong Authentication Achieved with a High Bit Count, User-Programmable Secret, and Input Challenge
  - Batteryless RF Communication
  - 4096 Bits of User EEPROM with User-Programmable Memory
  - Memory R/W Protection Options Including OTP/EPROM Emulation Mode
  - Unique Factory-Programmed 64-Bit Identification Number
  - Integrated 32-Byte SRAM Buffer Enables Faster HF-to-I²C Transactions
- Flexible Connection and Communication Capabilities Support a Wide Range of Applications
  - Programmable I/O (PIO) Can Be Configured as a Wake-Up or Monitoring/Control Signal
  - HF Standards ISO/IEC 15693 and 18000-3 MODE1 Compatible (13.56 MHz ±7kHz Carrier Frequency)
  - I²C Interface—Master/Slave Port Eliminates Host Microcontroller for Sensor-Tag Applications
  - Energy Harvesting V_{OUT} Pin for Powering External Components
  - Optional 3.3V Supply Voltage Fits Line and Battery-Powered Applications
  - -40°C to +85°C Operating Temperature Range
- Enables Robust Design
  - ±4kV HBM ESD Protection on PIO, ±2kV on All Other Pins

Typical Application Circuits



Typical Application Circuits **continued at end of data sheet.**

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

219-0038; Rev 3; 4/18

maxim integrated™

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND .....-0.5V to +4.0V
Maximum Current Into Any Pin Except AC1 or AC2 .....20mA
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
Supply Voltage	V_{CC}		2.97	3.3	3.63	V
Active Supply Current	I_{CCA}	(Note 3)			110	µA
Standby Supply Current	I_{CCS}				100	µA
Power-Up Time	t_{POR}				1	ms
SHA-256 ENGINE						
Computation Current	I_{CSHA}	V_{CC} = 3.63V (Note 4)			1.5	mA
Computation Time	t_{CSHA}	(Note 5)			2	ms
EEPROM						
Programming Current	I_{PROG}	V_{CC} = 3.63V (Note 4)			1.5	mA
Programming Time for a 32-Bit Page Block or Protection	t_{PROG}	(Note 6)			10	ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 7, 8)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Notes 9, 10, 11)	10			Years
PIO PIN						
Input Current with Input Voltage Between 0.1V_{CC} and 0.9V_{CCMAX}	I_{I_PIO}				1	µA
Input Low Voltage	V_{IL_PIO}		-0.3		0.4	V
Input High Voltage	V_{IH_PIO}		1.62			V
Output Low Voltage	V_{OL_PIO}	4mA sink current			0.4	V
RF PORT						
Carrier Frequency	f_C	(Note 12)	13.553	13.560	13.567	MHz
Internal Tuning Cap	C_{TUN}	f = 13.56 MHz (Note 13)		27.5		pF

Electrical Characteristics (continued)

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

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Operating Field	H_{ISO}	(Note 12)	150		5000	mA/m
Activation Field Strength	H_{MIN_10}	10%–30% modulation index (Note 13)		100		dBµA/m
Activation Field Strength	H_{MIN_100}	100% modulation index (Note 13)		101.2		dBµA/m
Write/SHA Field Strength	H_{WR}	(Notes 13, 14)		113		dBµA/m
V_{OUT} Field Strength	H_{MINOUT}	(Note 13)		122		dBµA/m
V_{OUT} Transition Time	t_{VOUT}	(Notes 13, 15)		250		µs
RF Access In Progress Time	t_{RFAIP}	(Notes 16)		1.1		ms
10% Carrier Modulation Index Min MI = (A - B)/(A + B)	CMI_10_{MIN}	(Notes 12, 13, 17)		10		%
10% Carrier Modulation Index Max MI = (A - B)/(A + B)	CMI_10_{MAX}	(Notes 12, 13)			30	%
100% Carrier Modulation Index MI = (A - B)/(A + B)	CMI_100	(Notes 12, 13)	95		100	%
10% Modulation Min Pulse Width	$t_{1\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		7.0		µs
10% Modulation Max Pulse Width	$t_{1\ MAX}$	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	µs
10% Modulation Min Low Time	$t_{2\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		7.0		µs
10% Modulation Max Low Time	$t_{2\ MAX}$	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	µs
10% Modulation Min Rise Time	$t_{3\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Note 13)	0			µs
10% Modulation Max Rise Time	$t_{3\ MAX}$	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		2.5		µs
100% Modulation Min Pulse Width	$t_{1\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		6.5		µs
100% Modulation Max Pulse Width	$t_{1\ MAX}$	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	µs
100% Modulation Min Low Time	$t_{2\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		6.5		µs
100% Modulation Max Low Time	$t_{2\ MAX}$	Refer to ISO 15693-2 Section 7.1 (Note 13)			9.44	µs
100% Modulation Min Rise Time	$t_{3\ MIN}$	Refer to ISO 15693-2 Section 7.1 (Note 13)	0			µs
100% Modulation Max Rise Time	$t_{3\ MAX}$	Refer to ISO 15693-2 Section 7.1 (Notes 13, 18)		3.0		µs
RF Timeout	$t_{RF\_TIMEOUT}$	(Note 13)		45		ms

Electrical Characteristics (continued)

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

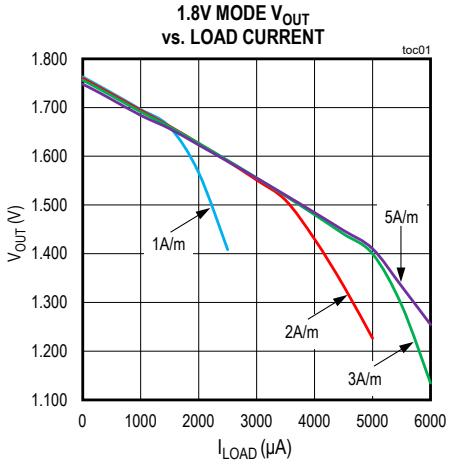
PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
SCL, SDA PINS (Note 21)							
Low Level Input Voltage	V_{IL}			-0.3		0.10 x V_{CC}	V
High Level Input Voltage	V_{IH}			0.8 x V_{CC}		V_{CC} + 0.3	V
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 13)			0.3		V
Output Low Voltage	V_{OL}	4mA sink current	T_A = -20°C to +85°C			0.10 x V_{CC}	V
			T_A = -40°C to -20°C			0.40	
Output Fall Time from V_{IHMIN} to V_{ILMAX} with a Bus Capacitance from 10pF to 400pF	t_{OF}	(Note 13)			150		ns
Input Current with Input Voltage Between 0.1V_{CC} and 0.9V_{CCMAX}	I_I	(Note 20)		-1		+1	µA
SCL Clock Frequency	f_{SCL}	(Notes 13, 21)				400	kHz
Master Mode Frequency	f_{MSTR}	f_C = 13.56MHz			53		kHz
I2C Timeout	$t_{I2C\_TIMEOUT}$	(Note 21)		25		50	ms
Hold Time (Repeated) START Condition.	$t_{HD:STA}$			0.6			µs
Low Period of the SCL Clock	t_{LOW}			1.3			µs
High Period of the SCL Clock	t_{HIGH}			0.6			µs
Setup Time for a Repeated START Condition	$t_{SU:STA}$			0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 13, 22, 23)				0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Notes 24)		100			ns
Setup Time for STOP Condition	$t_{SU:STO}$			0.6			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}			1.3			µs
Capacitive Load for Each Bus Line	C_B	(Notes 12, 13)				400	pF

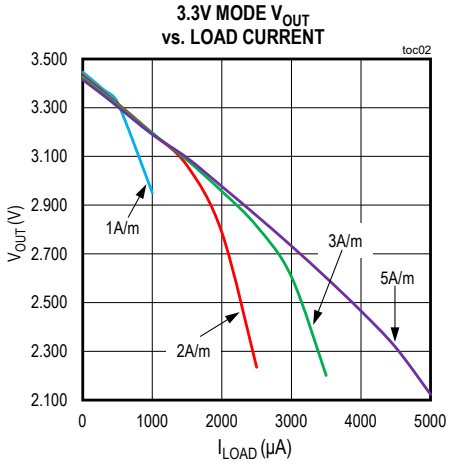
Electrical Characteristics (continued)

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

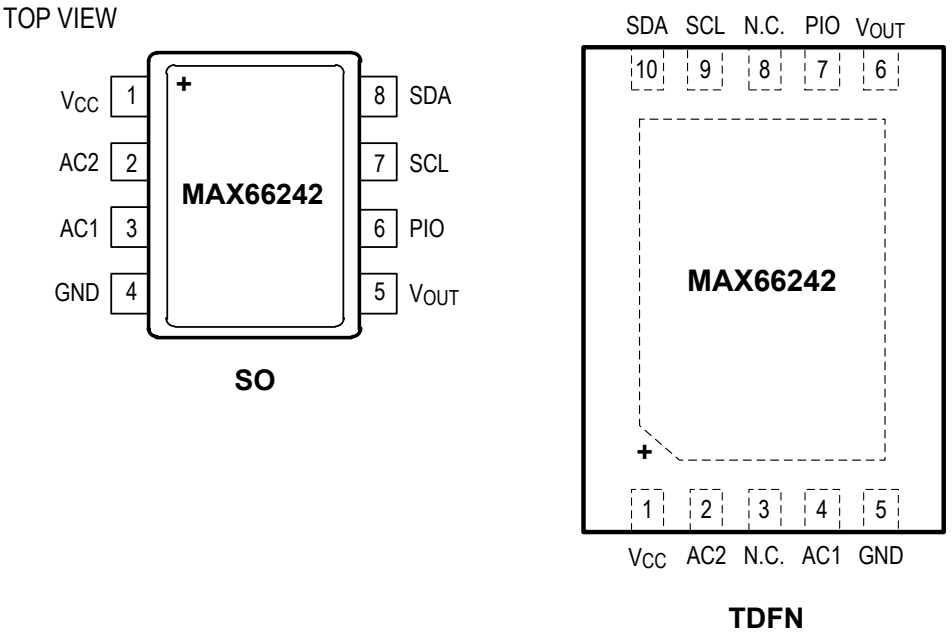
Note 2: Limits are 100% production tested at T_A = +25°C or T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are at 25°C.
Note 3: Operating current continuously reading the Memory/MAC Read/Write Register at 400kHz with no RF power.
Note 4: Refer to full data sheet.
Note 5: Refer to full data sheet.
Note 6: 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. For I2C commands the interval begins after the Acknowledge bit of the last data byte. The interval ends once the device's self-timed EEPROM write cycle is complete.
Note 7: Write-cycle endurance is tested in compliance with JESD47G.
Note 8: Not 100% production tested; guaranteed by reliability qualification.
Note 9: Data retention is tested in compliance with JESD47G.
Note 10: 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 11: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended.
Note 12: System requirement.
Note 13: Guaranteed by design, and/or characterization only. Not production tested.
Note 14: 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, Authenticated Set Protection RF Execute, and Configuration Write commands.
Note 15: Measured from V_{OUT} = 1.8V to V_{OUT} = 3.3V at 2.5A/m with a 0.1µF load.
Note 16: The t_{RFAIP} interval begins immediately after an EOF for a valid ISO15693 request frame and ends before SOF of the response frame. A pulse of width t_{RFAIP} will only occur only for Read/Write Scratchpad (writing) and Control Write.
Note 17: CMI_10 > 15% is suggested.
Note 18: Field strength between 350mA/m and 5A/m.
Note 19: All I2C timing values are referred to $V_{IH\ MIN}$ and $V_{IL\ MAX}$ levels.
Note 20: I/O pins of the MAX66242 do not obstruct SDA and SCL lines if V_{CC} and the RF fields are switched off.
Note 21: The minimum SCL clock frequency is limited by the I²C timeout feature. If SCL remains low longer than this interval, the MAX66242 behaves as though it has sensed a STOP condition. SDA has no affect on this timeout condition.
Note 22: The MAX66242 provides a hold time of at least 200ns for the SDA signal (referred to the V_{IHMIN} of the SCL signal) to bridge the undefined region of the falling edge of SCL.
Note 23: The master can provide a hold time of 0ns minimum when writing to the device.
Note 24: A fast-mode I2C-bus device can be used in a standard-mode I2C-bus system, but the requirement $t_{SU:DAT} \geq$ 250ns must then be met. This is automatically the case if the device does not stretch the LOW period of the SCL signal. If such a device does stretch the LOW period of the SCL signal, it must output the next data bit to the SDA line $t_{RMAX} + t_{SU:DAT}$ = 1000 + 250 = 1250ns (according to the standard-mode I2C-bus specification) before the SCL line is released.

Typical Operating Characteristics





Pin Configurations



Pin Descriptions

PIN		NAME	FUNCTION
SO	TDFN		
1	1	V_{CC}	Power-Supply Input
2	2	AC2	Antenna Connection
3	4	AC1	Antenna Connection
4	5	GND	Ground Reference
5	6	V_{OUT}	Energy Harvesting Pin. See the *PIO and Energy Harvesting Output* section.
6	7	PIO	Multipurpose Open-Drain Pin. See the *PIO and Energy Harvesting Output* section.
7	9	SCL	I²C Serial Clock Input
8	10	SDA	I²C Serial Data Input/Output
—	3, 8	N.C.	Not Connected

Detailed Description

The MAX66242 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. In addition to the RF interface, the part also has an I2C interface, which can operate as slave port or as master port.

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 MAX66242 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 MAX66242 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 MAX66242 is associated. Applications of the MAX66242 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 MAX66242. 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 seven categories: ISO 15693 generic commands, secret installation, memory access, protection setting, MAC computation, configuration and control with verification, and I2C master port operation. 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).

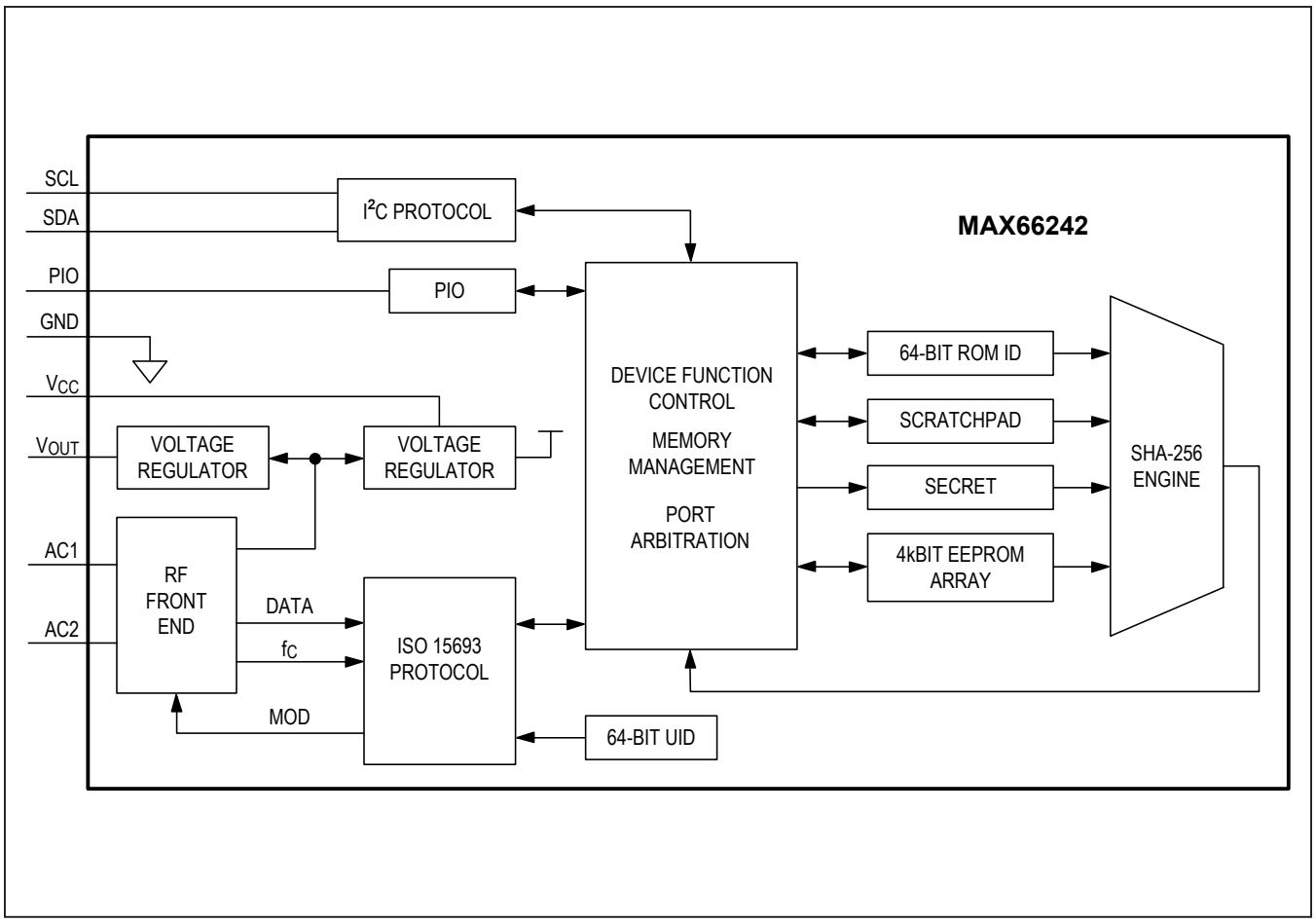


Figure 1. Block Diagram

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
	CONFIGURATION WRITE	MFGCODE, EEPROM CONFIGURATION BYTE
	CONFIGURATION READ	MFGCODE, EEPROM CONFIGURATION BYTE
	CONTROL WRITE	MFGCODE, SRAM CONTROL BYTE, PIO PORTS
	CONTROL READ	MFGCODE, SRAM CONTROL BYTE, PIO PORTS
	GET 1-WIRE ROM ID	MFGCODE, ROM ID
	PERIPHERAL TRANSACTION	MFGCODE, I²C PORT MASTER MODE
	WRITE AFI	AFI BYTE
	LOCK AFI	AFI LOCK STATUS
	WRITE DSFID	DSFID BYTE
	LOCK DSFID	DSFID LOCK STATUS

Figure 2. Commands Overview

Memory Resources

The memory of the MAX66242 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 MAX66242, 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 MAX66242 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 MAX66242 or written to the MAX66242 (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 MAX66242 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.
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), RF port only	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), RF port only	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 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 23 shows how the Reset to Ready, Stay Quiet, and Select commands respond when changing the transponder's state. Table 4 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

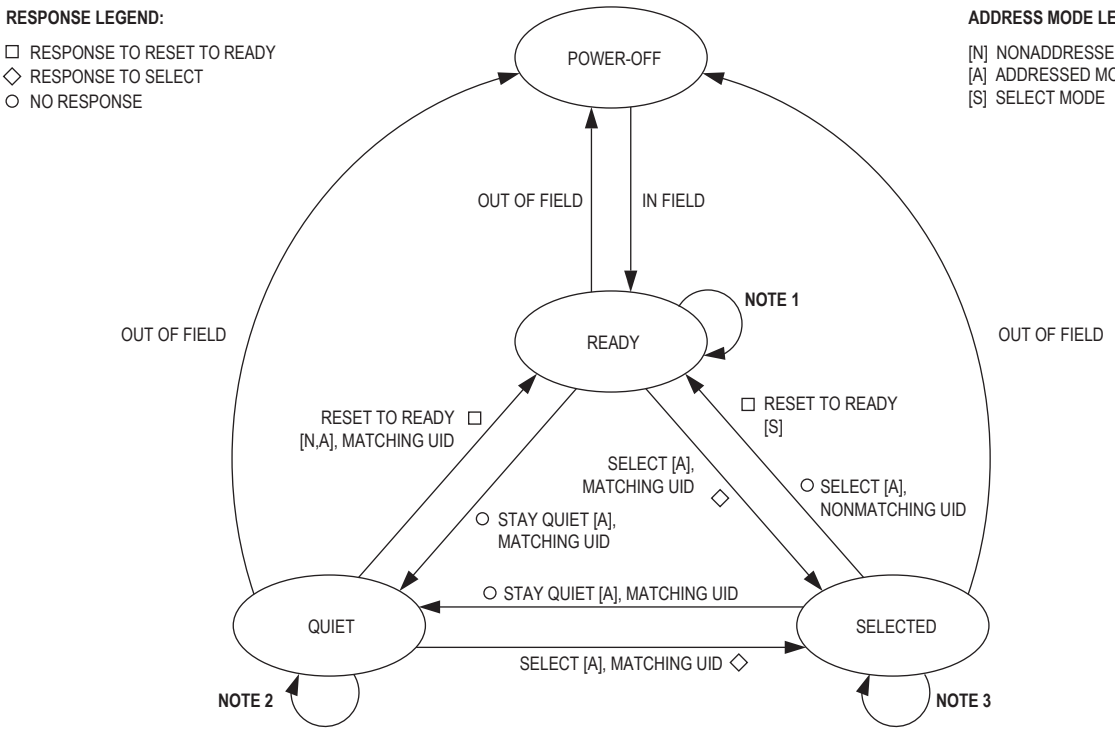
In this state, a transponder has enough power to perform any of its functions. The purpose of the quiet state is to silence transponders with which the reader does not want to communicate. Only commands sent with the addressed mode are processed. This way the reader can use the nonaddressed mode for 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 4. 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 23. ISO 15693 State Transition Diagram

I2C Interface Description

The block diagram in Figure 1 shows the relationships between the major control and memory sections of the MAX66242. The device has six main data components: 16 256-bit pages of user EEPROM, one 256-bit secret, protection-control/status memory, 512-bit SHA-256 engine, 64-bit ROM ID, and a 256-bit scratchpad. Figure 24 shows the applicable commands and the affected data fields.

Memory

The MAX66242 memory consists of three areas: 1) the directly accessible 256-byte address space with the scratchpad, protection status registers, ROM ID, and special function addresses, 2) the indirectly accessible user memory, and 3) the indirectly write-accessible secret memory of 32 bytes.

Figure 25 shows the organization of the directly accessible memory space, which begins at address 00h with the scratchpad. The register section begins at address 40h with the command register, which is followed by the MAC Read/Write Register. The protection status registers begin at address 50h (for memory pages) and 60h (secret). The ROM ID and several other factory programmable registers begin at address 68h. The scratchpad is implemented as volatile SRAM. The address range 50h and higher is nonvolatile.

The directly accessible memory space encompasses three types of memory: read/write, write-only, open read/indirect write, and read-only. To write to or read from the volatile scratchpad, one must begin at address 00h. Writing must take place in block of 4 bytes. The command register is write-only. The protection status registers can be read openly, but require the use of special function commands for writing. The ROM ID, manufacturer ID, and factory byte are read-only.

The EEPROM of the MAX66242 can be programmed using a factory preprogramming service. If this service is used, the Manufacturer ID is different from the 0000h default of unprogrammed parts.

Command Register (40h)

To install the secret, to read from or write to the user memory, or to set the user memory protection, or to compute and read a page MAC, the MAX66242 needs to receive a command from the I2C host. Commands are written one at a time to the Command register. Most commands consist of a command code and a parameter byte. The command code indicates the type of instruction and the position of the read pointer for the next I2C read-access. See the Function Commands section for details.

MAC Read/Write Register (41h)

For authenticated writing (memory, protection), the I2C host must provide a MAC to prove its authenticity to the MAX66242. To verify the MAX66242 authenticity, the Compute and Read Page MAC command delivers a MAC for the host to read. The MAC Read/Write Register is the single address access point for MAC.

Memory Protection Status Registers (50h–5Fh)

Each individual user memory page can be protected in several ways. Protections are activated through the Set Protection command or Authenticated Set Protection command (see the Function Commands section). The Memory Protection Status Registers (Table 41), one for each user memory page, allow the I2C host to verify the protection status. The Memory protection status register at address 50h corresponds to user memory page 0, etc.

MAX66242

AVAILABLE COMMANDS:	DATA FIELD AFFECTED:
WRITE MEMORY	USER MEMORY, PROTECTION SETTINGS
READ MEMORY	USER MEMORY, PROTECTION SETTINGS
SET PROTECTION	PROTECTION SETTINGS
INSTALL AND LOCK SECRET	SECRET, USER MEMORY, SCRATCHPAD AND LOCK STATUS
COMPUTE AND READ PAGE MAC	SECRET, USER MEMORY, SCRATCHPAD, 64-BIT ROM ID
AUTHENTICATED WRITE MEMORY	SECRET, USER MEMORY, 64-BIT ROM ID, PROTECTION SETTINGS
AUTHENTICATED SET PROTECTION	SECRET, MEMORY PAGE NUMBER, PROTECTION SETTINGS, 64-BIT ROM ID
CONFIGURATION WRITE	EEPROM CONFIGURATION BYTE
CONFIGURATION READ	EEPROM CONFIGURATION BYTE
CONTROL WRITE	SRAM CONTROL BYTE
CONTROL READ	SRAM CONTROL BYTE

Figure 24. Commands Overview

ABRIDGED DATA SHEET

MAX66242

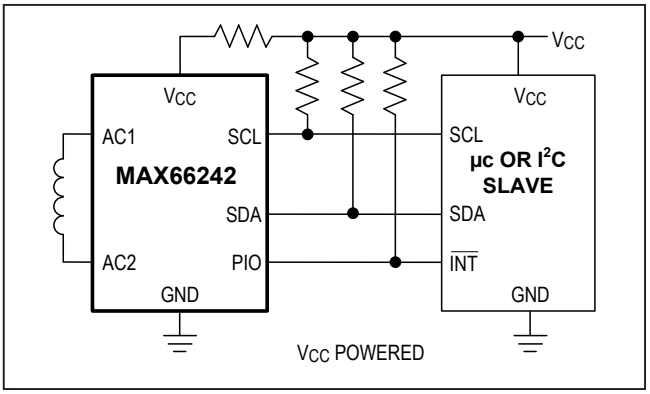
DeepCover Secure Authenticator with ISO 15693, I²C, SHA-256, and 4Kb User EEPROM

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAX66242ESA+	-40°C to +85°C	8 SO
MAX66242ESA+T	-40°C to +85°C	8 SO (2.5k pcs)
MAX66242ETB+	-40°C to +85°C	10 TDFN
MAX66242ETB+T	-40°C to +85°C	10 TDFN (2.5k pcs)
MAX66242E/W+†	-40°C to +85°C	AU bumped, tested, diced wafer
MAX66242/W+†	-40°C to +85°C	Tested wafer

+Denotes a lead(Pb)-free/RoHS-compliant package.
T = Tape and reel.
†Contact factory for further details.

Typical Application Circuits (continued)



Package Information

For the latest package outline information and land patterns (footprints), go to **www.maximintegrated.com/packages**. Note that a "+", "#", or "-" in the package code indicates RoHS status only. Package drawings may show a different suffix character, but the drawing pertains to the package regardless of RoHS status.

PACKAGE TYPE	PACKAGE CODE	OUTLINE NO.	LAND PATTERN NO.
8 SO (150 mils)	S8+2	21-0041	90-0096
10 TDFN (3mm x 4mm)	T1034N+1	21-0268	90-0247
Wafer	—	—	—

Errata

ISO 15693-3 Section 9.1 specifies that if the VICC detects a carrier modulation during time t_1, it shall reset its t_1 timer and wait for a further time t_1 before starting to transmit its response to a VCD request or to switch to the next slot when in an inventory process. The MAX66242 is not compliant with this specification.

ISO15693-3 Section 9.4.2 specifies that during an inventory process, when the VCD has received no VICC response, it shall wait a time t_3 before sending a subsequent EOF to switch to the next slot. If the VCD sends a 100% modulated EOF, the minimum value of t_3 is 4384/fc (323.3µs) + tsof. The MAX66242 is not compliant with this specification. The MAX66242 requires a minimum t_3 = 4384/fc (323.3µs) + tnrt + t2min, where tsof is the time duration for a VICC to transmit an SOF to the VCD, and tnrt is the nominal response time of a VICC. tnrt and tsof are dependent on the VICC-to-VCD data rate and subcarrier modulation mode.

The peripheral transaction command responds with an A0h error when Address_Flag = 0.

For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Security ICs / Authentication ICs ***category:***

Click to view products by Maxim ***manufacturer:***

Other Similar products are found below :

RJM8L151F6P6R AT97SC3204T-X2A1B-10 SLS32AIA020A4USON10XTMA2 AT97SC3205T-G3M4C-00 AT97SC3205T-H3M4C-20 AT97SC3204-U4A14-20 AT97SC3205T-H3M4C20B AT97SC3205-X3A12-10 AT97SC3204-U2MA-20 AT97SC3204-X2A1A-10 ATAES132-SH-EQ ATECC508A-MAHDA-S DS2401+ DS1990A-F3+ DS1990A-F5+ DS2401P+T&R DS2401Z+T&R DS2411P+ DS2411P+T&R ATSHA204-TH-CZ-T DS28CM00R-A00+T DS28C22Q+T ATTPM20P-G3MA1-10-B HCS515-IP HCS515P MCS3122-I/ST MIKROE-3047 ATECC508A-SSHDA-T ATSHA204A-SSHDA-B ATAES132A-SHEQ-B ATECC108A-SSHCZ-B ATSHA204A-SSHDA-T W74M32FVSSIQ IPL-CHP1.8V ATSHA204A-STUCZ-T DS2411R+T&R RJM8L151K8Q6Y CW3802 RJGT102WDP8 FM15160 508-03 RJGT102WDT6 RJMU401FHO ATECC108A-RBHCZ-T IPL-CHP 404726X AT88SC0808CA-Y6H-T AT88SA102S-SH-T MAX66240ESA+