*Click **here** to ask an associate for production status of specific part numbers.*

MAX66250

ISO 15693, SHA3-256, 256-Bit User EEPROM Secure Authenticator

General Description

The MAX66250 secure authenticator combines FIPS 202-compliant Secure Hash Algorithm (SHA-3) challenge and response authentication with secured EEPROM.

The device provides a core set of cryptographic tools derived from integrated blocks including a SHA-3 engine, 256 bits of secured user EEPROM, a decrement-only counter and a unique 64-bit ROM identification number (ROM ID). The unique ROM ID is used as a fundamental input parameter for cryptographic operations and serves as an electronic serial number within the application. The device communicates over an RF interface compliant with ISO/IEC 15693.

Applications

- Medical Tools/Accessories Authentication and Calibration
- Printer Cartridge Configuration and Monitoring
- System Intellectual Property Protection
- NFC-Enabled Embedded Systems
- Asset Tracking
- Access Control
- Driver Identification
- E-Cash

Request MAX66250 Security User Guide

Benefits and Features

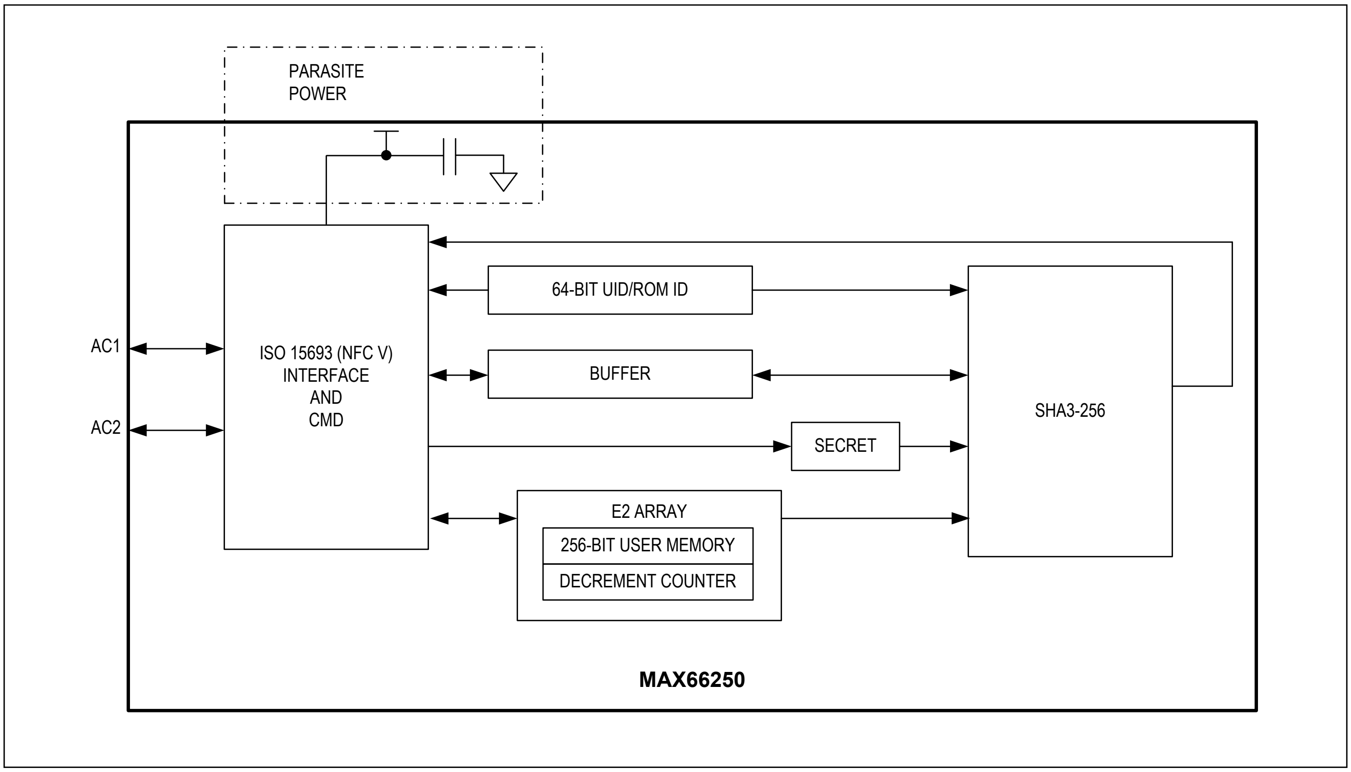
- Robust Countermeasures Protect against Security Attacks
  - All Stored Data Cryptographically Protected from Discovery
- Efficient Secure Hash Algorithm to Authenticate Peripherals
  - FIPS 202-Compliant SHA-3 Algorithm for Challenge/Response Authentication
  - FIPS 198-Compliant Keyed-Hash Message Authentication Code (HMAC)
- Supplemental Features Enable Easy Integration into End Applications
  - 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
  - Secure Storage for Secrets
  - 256 Bits of Secure EEPROM for User Data
  - ISO/IEC 15693: up to 52.97kbps
  - Unique and Unalterable Factory-Programmed 64-Bit Identification Number (ROM ID) with Corresponding UID per ISO/IEC 15693

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

Ordering Information appears at end of data sheet.

19-101591; Rev 0; 7/22

Simplified Block Diagram



Absolute Maximum Ratings

Voltage Range on Any Pin Relative to IC GND........ -0.5V to +4V
Maximum RMS Current, AC1 to AC2 .... 30mA
Maximum Incident Magnetic Field Strength (ISO/IEC 7810 ID-1 antenna aperture) 12A/m
Operating Temperature Range ....-40°C to +85°C
Junction Temperature .... +150°C
Storage Temperature Range ....-55°C to +125°C
Lead temperature (soldering, 10 seconds) .... +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 Information

SO

Package Code	S8+2
Outline Number	**21-0041**
Land Pattern Number	**90-0096**
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	170°C/W
Junction to Case (θ_{JC})	40°C/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	136°C/W
Junction to Case (θ_{JC})	38°C/W

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 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

(Limits are 100% tested at T_A = +25°C and T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Specifications marked "GBD" are guaranteed by design and not production tested. Typical values are at +25°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Power-Up Time	t_{POR}				1	ms
SHA3-256 ENGINE						
Computation Time	t_{CMP}				35	ms
EEPROM						
Read Memory Time	t_{RM}				10	ms
Write Memory Time	t_{WM}				65	ms
Short Write Memory Time	t_{WMS}				15	ms
Write/Erase Cycling Endurance	NCY	T_A = +85°C (*Note 1*, *Note 2*, *Note 3*)	100k			
Data Retention	tDR	T_A = +85°C (*Note 4*, *Note 5*, *Note 6*)	10			years
RF INTERFACE						
Carrier Frequency	f_C	*Note 7*	13.553	13.56	13.567	MHz
Internal Tuning Cap	CTUN	f = 13.56MHz (*Note 8*)		21.5		pF
Operating Field	HISO	*Note 7*	150		5000	mA/m

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25°C and T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Specifications marked "GBD" are guaranteed by design and not production tested. Typical values are at +25°C.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Activation Field Strength	HMIN	Note 8		75		mA/m
Write/SHA Field Strength	HWR	Note 8, Note 9		265		mA/m
10% Carrier Modulation Index MI = (A - B)/(A + B)	CMI_10	Note 7	10		30	%
100% Carrier Modulation Index MI = (A - B)/(A + B)	CMI_100	Note 7	95		100	%
Modulation Pulse Width	t1 min	Refer to ISO 15693-2 Section 7.1 (Note 8)		6.00		µs
	t1 max	Refer to ISO 15693-2 Section 7.1 (Note 8)		9.44		
10% Modulation Low Time	t2_10 min	Refer to ISO 15693-2 Section 7.1 (Note 8)		3.00		µs
100% Modulation Low Time	t2_100 min	Refer to ISO 15693-2 Section 7.1 (Note 8)		2.10		µs
	t2 max	Refer to ISO 15693-2 Section 7.1 (Note 8)			t1	
Modulation Rise Time to Full Amplitude	t3 min	Refer to ISO 15693-2 Section 7.1 (Note 8)		0.00		µs
Modulation Rise Time To Full Amplitude	t3 max	Refer to ISO 15693-2 Section 7.1 (Note 8)		4.50		µs

Note 1: Write-cycle endurance is tested in compliance with JESD47H.

Note 2: Not 100% production tested; guaranteed by reliability qualification.

Note 3: 10k for Write AFI, Lock AFI, Write DSFID, and Lock DSFID commands

Note 4: Data retention is tested in compliance with JESD47H.

Note 5: 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.

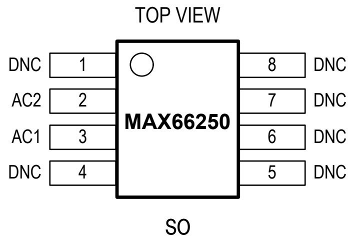
Note 6: EEPROM writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended.

Note 7: System requirement.

Note 8: Guaranteed by design and/or characterization only. Not production tested.

Note 9: Applies to commands utilizing the SHA3-256 engine as well as EEPROM and scratchpad operations (See the *MAX66250 Security User Guide* for details).

Pin Configuration



Pin Description

PIN	NAME	FUNCTION	TYPE
1, 4, 5, 6, 7, 8	DNC	Do Not Connect	I/O
			I/O
			I/O
			I/O
			I/O
			I/O
2	AC2	Antenna Connection	I/O
3	AC1	Antenna Connection	I/O

Detailed Description

The MAX66250 integrates Analog Devices' DeepCover® capability to protect all device-stored data from invasive discovery. In addition to the SHA-3 engine for signatures and authenticated writes, the MAX66250 includes a 256-bit EEPROM for user memory, SHA-3 secret storage, 17-bit decrement counter, and control registers. The device communicates through an ISO/IEC 15693 interface.

Design Resource Overview

Operation of the MAX66250 involves the use of device EEPROM and execution of device function commands. The following sections provide an overview, including the decrement counter. Refer to the *MAX66250 Security User Guide* for details.

Memory

A secured EEPROM array provides SHA-3 secret storage, along with a decrement counter, and/or general-purpose, user-programmable memory. Depending on the memory space, there are either default or user-programmable options to set protection modes.

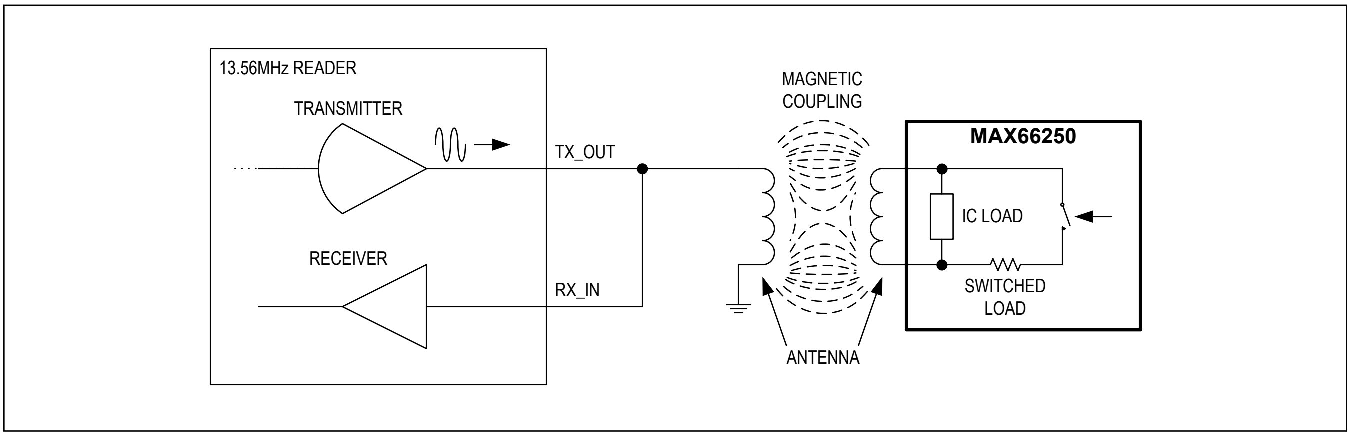
Decrement Counter

The optional 17-bit decrement counter can be written one time on a page of memory. A dedicated device function command is used to decrement the count value by one with each call. Once the count value reaches a value of 0, no additional decrements are possible.

ROM-ID

Each MAX66250 contains a unique, 64-bit long ROM ID that can be incorporated into HMAC calculations. Information from the ROM ID is reassembled into a unique ID (UID) that is compatible with ISO 15693.

Typical Application Circuit



Ordering Information

PART NUMBER	TEMP RANGE	PIN-PACKAGE
MAX66250ESA+	-40°C to +85°C	8 SO
MAX66250ESA+T	-40°C to +85°C	8 SO (2.5k pcs)

+ Denotes a lead(Pb)-free/RoHS-compliant package.

T Denotes tape-and-reel.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	7/22	Initial release	—

Information furnished by Analog Devices is believed to be accurate and reliable. However, no responsibility is assumed by Analog Devices for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implication or otherwise under any patent or patent rights of Analog Devices. Trademarks and registered trademarks are the property of their respective owners.