

## DS28E25

# DeepCover Secure Authenticator with 1-Wire 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 (DS28E25) combines crypto-strong, bidirectional, secure challenge-and-response authentication functionality with an implementation based on the FIPS 180-3-specified Secure Hash Algorithm (SHA-256). A 4Kb user-programmable EEPROM array provides nonvolatile storage of application data and additional protected memory holds a read-protected secret for SHA-256 operations and settings for user memory control. Each device has its own guaranteed unique 64-bit ROM identification number (ROM ID) that is factory programmed into the chip. This unique ROM ID is used as a fundamental input parameter for cryptographic operations and also serves as an electronic serial number within the application. A bidirectional security model enables two-way authentication between a host system and slave-embedded DS28E25. Slave-to-host authentication is used by a host system to securely validate that an attached or embedded DS28E25 is authentic. Host-to-slave authentication is used to protect DS28E25 user memory from being modified by a non-authentic host. The SHA-256 message authentication code (MAC), which the DS28E25 generates, is computed from data in the user memory, an on-chip secret, a host random challenge, and the 64-bit ROM ID. The DS28E25 communicates over the single-contact 1-Wire® bus at overdrive speed. The communication follows the 1-Wire protocol with the ROM ID acting as node address in the case of a multiple-device 1-Wire network.

### Applications

- Authentication of Network-Attached Appliances
- Printer Cartridge ID/Authentication
- Reference Design License Management
- System Intellectual Property Protection
- Sensor/Accessory Authentication and Calibration
- Secure Feature Setting for Configurable Systems
- Key Generation and Exchange for Cryptographic Systems

DeepCover is a trademark and 1-Wire is a registered trademark of Maxim Integrated Products, Inc.

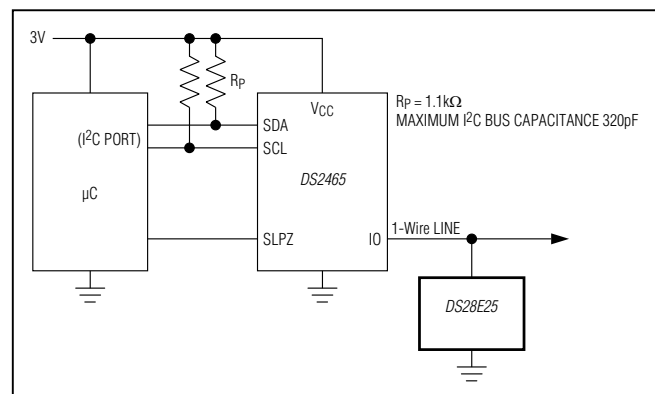
For related parts and recommended products to use with this part, refer to: [www.maximintegrated.com/DS28E25.related](http://www.maximintegrated.com/DS28E25.related)

**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](http://www.maximintegrated.com).**

### Features

- ◆ Symmetric Key-Based Bidirectional Secure Authentication Model Based on SHA-256
- ◆ 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 Partitioned Into 16 Pages of 256 Bits
- ◆ User-Programmable and Irreversible EEPROM Protection Modes Including Authentication, Write and Read Protect, and OTP/EPROM Emulation
- ◆ Unique, Factory-Programmed 64-Bit Identification Number
- ◆ Single-Contact 1-Wire Interface Communicates with Host at Up to 76.9kbps
- ◆ Operating Range: 3.3V ±10%, -40°C to +85°C
- ◆ Low-Power 5µA (typ) Standby
- ◆ ±8kV Human Body Model ESD Protection (typ)
- ◆ 2-Pin SFN, 2-Pin TO-92, 6-Pin TDFN, and 6-Pin TSOC Packages

### Typical Application Circuit



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

## DS28E25

# DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM

### ABSOLUTE MAXIMUM RATINGS

IO Voltage Range to GND.....	-0.5V to 4.0V	Lead Temperature (soldering, 10s)	
IO Sink Current.....	20mA	TO-92, TSOC, TDFN .....	+300°C
Operating Temperature Range .....	-40°C to +85°C	Soldering Temperature (reflow)	
Junction Temperature .....	+150°C	TO-92 .....	+250°C
Storage Temperature Range.....	-55°C to +125°C	TSOC, TDFN .....	+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.

### ELECTRICAL CHARACTERISTICS

(T<sub>A</sub> = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
<b>IO PIN: GENERAL DATA</b>						
1-Wire Pullup Voltage	V <sub>PUP</sub>	(Note 2)	2.97		3.63	V
1-Wire Pullup Resistance	R <sub>PUP</sub>	V <sub>PUP</sub> = 3.3V ± 10% (Note 3)	300		1500	Ω
Input Capacitance	C <sub>IO</sub>	(Notes 4, 5)		1500		pF
Input Load Current	I <sub>L</sub>	IO pin at V <sub>PUP</sub>		5	19.5	μA
High-to-Low Switching Threshold	V <sub>TL</sub>	(Notes 6, 7)		0.65 x V <sub>PUP</sub>		V
Input Low Voltage	V <sub>IL</sub>	(Notes 2, 8)			0.3	V
Low-to-High Switching Threshold	V <sub>TH</sub>	(Notes 6, 9)		0.75 x V <sub>PUP</sub>		V
Switching Hysteresis	V <sub>HY</sub>	(Notes 6, 10)		0.3		V
Output Low Voltage	V <sub>OL</sub>	I <sub>OL</sub> = 4mA (Note 11)			0.4	V
Recovery Time	t <sub>REC</sub>	R <sub>PUP</sub> = 1500Ω (Notes 2, 12)	5			μs
Time-Slot Duration	t <sub>SLOT</sub>	(Notes 2, 13)	13			μs
<b>IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE</b>						
Reset Low Time	t <sub>RSTL</sub>	(Note 2)	48		80	μs
Reset High Time	t <sub>RSTH</sub>	(Note 14)	48			μs
Presence-Detect Sample Time	t <sub>MSP</sub>	(Notes 2, 15)	8		10	μs
<b>IO PIN: 1-Wire WRITE</b>						
Write-Zero Low Time	t <sub>W0L</sub>	(Notes 2, 16)	8		16	μs
Write-One Low Time	t <sub>W1L</sub>	(Notes 2, 16)	1		2	μs
<b>IO PIN: 1-Wire READ</b>						
Read Low Time	t <sub>RL</sub>	(Notes 2, 17)	1		2 - δ	μs
Read Sample Time	t <sub>MSR</sub>	(Notes 2, 17)	t <sub>RL</sub> + δ		2	μs
<b>EEPROM</b>						
Programming Current	I <sub>PROG</sub>	V <sub>PUP</sub> = 3.63V (Notes 5, 18)			1	mA
Programming Time for a 32-Bit Segment or Page Protection	t <sub>PRD</sub>	<b>Refer to the full data sheet.</b>				ms
Programming Time for the Secret	t <sub>PRS</sub>					ms
Write/Erase Cycling Endurance	N <sub>CY</sub>	T <sub>A</sub> = +85°C (Notes 21, 22)	100k			—
Data Retention	t <sub>DR</sub>	T <sub>A</sub> = +85°C (Notes 23, 24, 25)	10			Years

## DS28E25

# DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM

### ELECTRICAL CHARACTERISTICS (continued)

( $T_A = -40^{\circ}\text{C}$  to  $+85^{\circ}\text{C}$ , unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
<b>SHA-256 ENGINE</b>						
Computation Current	$I_{\text{CSHA}}$	<b>Refer to the full data sheet.</b>				mA
Computation Time	$t_{\text{CSHA}}$					ms

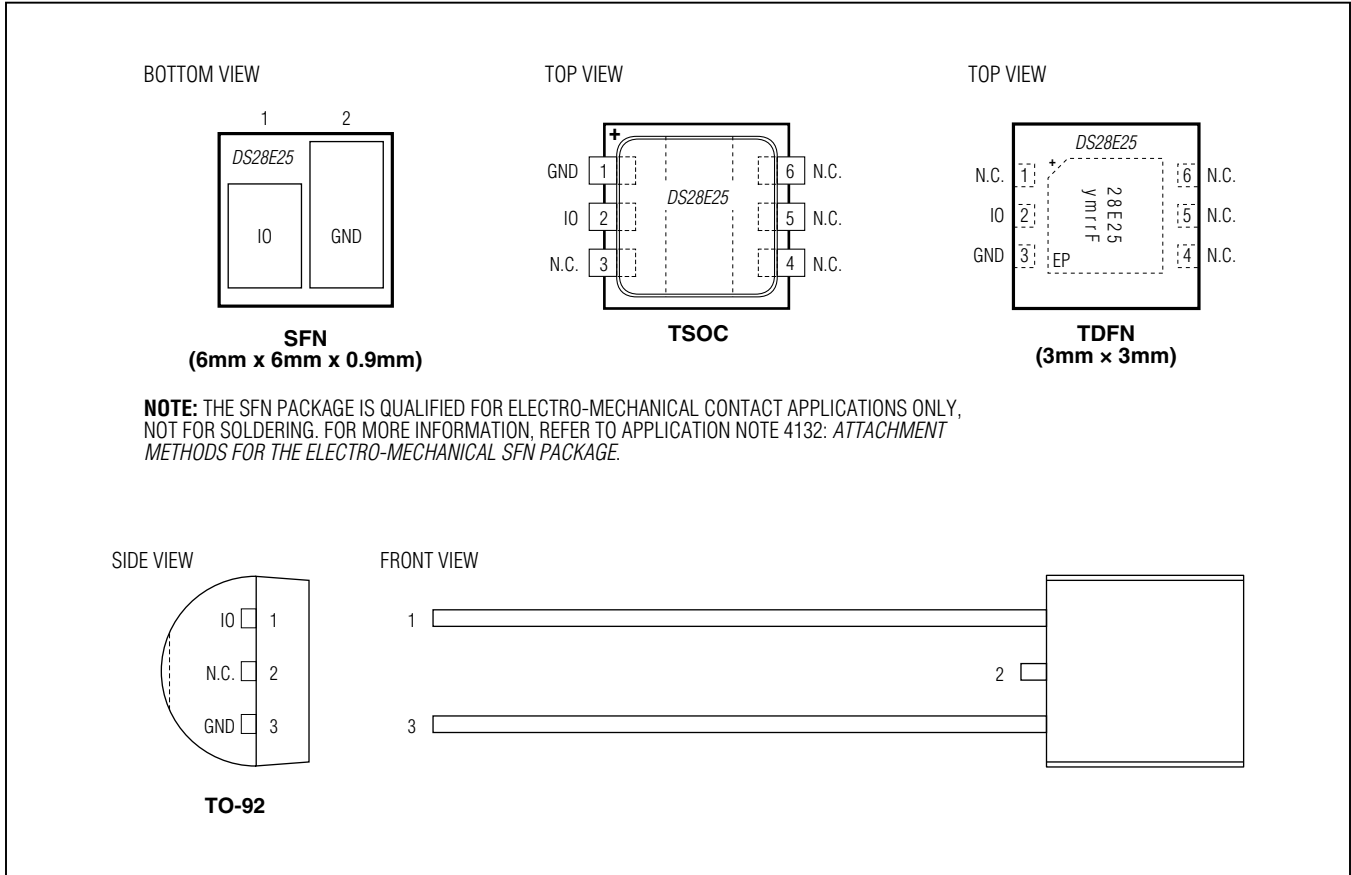
- Note 1:** Limits are 100% production tested at  $T_A = +25^{\circ}\text{C}$  and/or  $T_A = +85^{\circ}\text{C}$ . Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are not guaranteed.
- Note 2:** System requirement.
- Note 3:** Maximum allowable pullup resistance is a function of the number of 1-Wire devices in the system and 1-Wire recovery times. The specified value here applies to systems with only one device and with the minimum 1-Wire recovery times.
- Note 4:** Typical value represents the internal parasite capacitance when  $V_{\text{PUP}}$  is first applied. Once the parasite capacitance is charged, it does not affect normal communication.
- Note 5:** Guaranteed by design and/or characterization only; not production tested.
- Note 6:**  $V_{\text{TL}}$ ,  $V_{\text{TH}}$ , and  $V_{\text{HY}}$  are a function of the internal supply voltage, which is a function of  $V_{\text{PUP}}$ ,  $R_{\text{PUP}}$ , 1-Wire timing, and capacitive loading on IO. Lower  $V_{\text{PUP}}$ , higher  $R_{\text{PUP}}$ , shorter  $t_{\text{REC}}$ , and heavier capacitive loading all lead to lower values of  $V_{\text{TL}}$ ,  $V_{\text{TH}}$ , and  $V_{\text{HY}}$ .
- Note 7:** Voltage below which, during a falling edge on IO, a logic-zero is detected.
- Note 8:** The voltage on IO must be less than or equal to  $V_{\text{ILMAX}}$  at all times when the master is driving IO to a logic-zero level.
- Note 9:** Voltage above which, during a rising edge on IO, a logic-one is detected.
- Note 10:** After  $V_{\text{TH}}$  is crossed during a rising edge on IO, the voltage on IO must drop by at least  $V_{\text{HY}}$  to be detected as logic-zero.
- Note 11:** The I-V characteristic is linear for voltages less than 1V.
- Note 12:** Applies to a single device attached to a 1-Wire line.
- Note 13:** Defines maximum possible bit rate. Equal to  $1/(t_{\text{WOLMIN}} + t_{\text{RECMIN}})$ .
- Note 14:** An additional reset or communication sequence cannot begin until the reset high time has expired.
- Note 15:** Interval after  $t_{\text{RSTL}}$  during which a bus master can read a bus 0 on IO if there is a DS28E25 present. The power-up presence detect pulse could be outside this interval, but will be complete within 2ms after power-up.
- Note 16:**  $\epsilon$  in [Figure 11](#) represents the time required for the pullup circuitry to pull the voltage on IO up from  $V_{\text{IL}}$  to  $V_{\text{TH}}$ . The actual maximum duration for the master to pull the line low is  $t_{\text{W1LMAX}} + t_{\text{F}} - \epsilon$  and  $t_{\text{W0LMAX}} + t_{\text{F}} - \epsilon$ , respectively.
- Note 17:**  $\delta$  in [Figure 11](#) represents the time required for the pullup circuitry to pull the voltage on IO up from  $V_{\text{IL}}$  to the input-high threshold of the bus master. The actual maximum duration for the master to pull the line low is  $t_{\text{RLMAX}} + t_{\text{F}}$ .
- Note 18:** Current drawn from IO during the EEPROM programming interval or SHA-256 computation. The pullup circuit on IO during the programming interval or SHA-256 computation should be such that the voltage at IO is greater than or equal to 2.0V.
- Note 19: Refer to the full data sheet.**
  
- Note 20: Refer to the full data sheet.**
  
- Note 21:** Write-cycle endurance is tested in compliance with JESD47G.
- Note 22:** Not 100% production tested; guaranteed by reliability monitor sampling.
- Note 23:** Data retention is tested in compliance with JESD47G.
- Note 24:** 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 25:** EEPROM writes can become nonfunctional after the data retention time is exceeded. Long-term storage at elevated temperatures is not recommended.
- Note 26: Refer to the full data sheet.**

# ABRIDGED DATA SHEET

## DS28E25

### DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM

#### Pin Configurations



#### Pin Descriptions

PIN				NAME	FUNCTION
SFN	TO-92	TSOC	TDFN-EP		
2	3	1	3	GND	Ground Reference
1	1	2	2	IO	1-Wire Bus Interface. Open-drain signal that requires an external pullup resistor.
—	2	3, 4, 5, 6	1, 4, 5, 6	N.C.	Not Connected
—	—	—	—	EP	Exposed Pad (TDFN only). Solder evenly to the board's ground plane for proper operation. Refer to Application Note 3273: <i>Exposed Pads: A Brief Introduction</i> for additional information.

## DS28E25

### DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM

**Note to readers:** This document is an abridged version of the full data sheet. Additional device information is available only in the full version of the data sheet. To request the full data sheet, go to [www.maximintegrated.com/DS28E25](http://www.maximintegrated.com/DS28E25) and click on **Request Full Data Sheet**.

#### Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28E25G+T	-40°C to +85°C	2 SFN (2.5k pcs)
DS28E25+	-40°C to +85°C	2 TO-92
DS28E25P+	-40°C to +85°C	6 TSOC
DS28E25P+T	-40°C to +85°C	6 TSOC (4k pcs)
DS28E25Q+T	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)

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

T = Tape and reel.

\*EP = Exposed pad.

#### Package Information

For the latest package outline information and land patterns (footprints), go to [www.maximintegrated.com/packages](http://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.
2 SFN	G266N+1	<a href="#">21-0390</a>	—
2 TO-92	Q2+1	<a href="#">21-0249</a>	—
6 TSOC	D6+1	<a href="#">21-0382</a>	<a href="#">90-0321</a>
6 TDFN-EP	T633+2	<a href="#">21-0137</a>	<a href="#">90-0058</a>



Maxim Integrated cannot assume responsibility for use of any circuitry other than circuitry entirely embodied in a Maxim Integrated product. No circuit patent licenses are implied. Maxim Integrated reserves the right to change the circuitry and specifications without notice at any time. The parametric values (min and max limits) shown in the Electrical Characteristics table are guaranteed. Other parametric values quoted in this data sheet are provided for guidance.