

DS28EL22

DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb 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 (DS28EL22) 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 2Kb user-programmable EEPROM array provides non-volatile 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 DS28EL22. Slave-to-host authentication is used by a host system to securely validate that an attached or embedded DS28EL22 is authentic. Host-to-slave authentication is used to protect DS28EL22 user memory from being modified by a nonauthentic host. The SHA-256 message authentication code (MAC), which the DS28EL22 generates, is computed from data in the user memory, an on-chip secret, a host random challenge, and the 64-bit ROM ID. The DS28EL22 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

Ordering Information appears at end of data sheet.

DeepCover and 1-Wire are registered trademarks of Maxim Integrated Products, Inc.

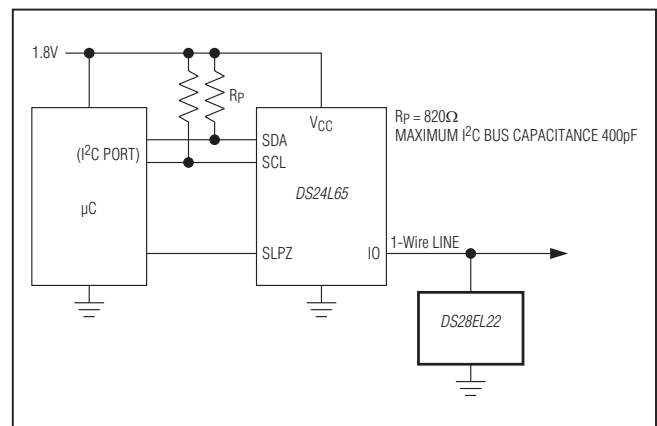
For related parts and recommended products to use with this part, refer to: www.maximintegrated.com/DS28EL22.related

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.

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**
- ◆ **2048 Bits of User EEPROM Partitioned Into 8 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: 1.8V ±5%, -40°C to +85°C**
- ◆ **Low-Power 5µA (typ) Standby**
- ◆ **±8kV Human Body Model ESD Protection (typ)**
- ◆ **6-Pin TDFN Package**

Typical Application Circuit



DS28EL22

DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM

ABSOLUTE MAXIMUM RATINGS

IO Voltage Range to GND..... -0.5V to 4.0V
 IO Sink Current.....20mA
 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.

ELECTRICAL CHARACTERISTICS

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V _{PUP}	(Note 2)	1.71		1.89	V
1-Wire Pullup Resistance	R _{PUP}	V _{PUP} = 1.8V ± 5% (Note 3)	300		750	Ω
Input Capacitance	C _{IO}	(Notes 4, 5)		1500		pF
Input Load Current	I _L	IO pin at V _{PUP}		5	19.5	μA
High-to-Low Switching Threshold	V _{TL}	(Notes 6, 7)		0.65 × V _{PUP}		V
Input Low Voltage	V _{IL}	(Notes 2, 8)			0.3	V
Low-to-High Switching Threshold	V _{TH}	(Notes 6, 9)		0.75 × V _{PUP}		V
Switching Hysteresis	V _{HY}	(Notes 6, 10)		0.3		V
Output Low Voltage	V _{OL}	I _{OL} = 4mA (Note 11)			0.4	V
Recovery Time	t _{REC}	R _{PUP} = 750Ω (Notes 2, 12)	5			μs
Time-Slot Duration	t _{SLOT}	(Notes 2, 13)	13			μs
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time	t _{RSTL}	(Note 2)	48		80	μs
Reset High Time	t _{RSTH}	(Note 14)	48			μs
Presence-Detect Sample Time	t _{MSP}	(Notes 2, 15)	8		10	μs
IO PIN: 1-Wire WRITE						
Write-Zero Low Time	t _{W0L}	(Notes 2, 16)	8		16	μs
Write-One Low Time	t _{W1L}	(Notes 2, 16)	1		2	μs
IO PIN: 1-Wire READ						
Read Low Time	t _{RL}	(Notes 2, 17)	1		2 - δ	μs
Read Sample Time	t _{MSR}	(Notes 2, 17)	t _{RL} + δ		2	μs
EEPROM						
Programming Current	I _{PROG}	V _{PUP} = 1.89V (Notes 5, 18)			1	mA
Programming Time for a 32-Bit Segment or Page Protection	t _{PRD}	(Note 19)			10	ms
Programming Time for the Secret	t _{PRS}	(Note 20)			200	ms
Write/Erase Cycling Endurance	N _{CY}	T _A = +85°C (Notes 21, 22)	100k			—
Data Retention	t _{DR}	T _A = +85°C (Notes 23, 24, 25)	10			Years

DS28EL22

DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb 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
SHA-256 ENGINE						
Computation Current	I_{CSHA}	$V_{\text{PUP}} = 1.89\text{V}$ (Notes 5, 18)			1	mA
Computation Time	t_{CSHA}	(Notes 5, 26)			3	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_{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_{TL} , V_{TH} , and V_{HY} are a function of the internal supply voltage, which is a function of V_{PUP} , R_{PUP} , 1-Wire timing, and capacitive loading on IO. Lower V_{PUP} , higher R_{PUP} , shorter t_{REC} , and heavier capacitive loading all lead to lower values of V_{TL} , V_{TH} , and V_{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_{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_{TH} is crossed during a rising edge on IO, the voltage on IO must drop by at least V_{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_{RSTL} during which a bus master can read a logic 0 on IO if there is a DS28EL22 present. The power-up presence detect pulse could be outside this interval. See the [Typical Operating Characteristics](#) for details.
- Note 16:** ϵ in [Figure 11](#) represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{TH} . The actual maximum duration for the master to pull the line low is $t_{\text{W1LMAX}} + t_{\text{F}} - \epsilon$ and $t_{\text{WOLMAX}} + t_{\text{F}} - \epsilon$, respectively.
- Note 17:** δ in [Figure 11](#) represents the time required for the pullup circuitry to pull the voltage on IO up from V_{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 and computation interval should be such that the voltage at IO is greater than or equal to V_{PUPMIN} . A low-impedance bypass of R_{PUP} activated during programming and computation is the recommended way to meet this requirement.
- Note 19:** The t_{PRD} interval begins immediately after the trailing rising edge on IO for the last time slot of the release byte for a valid Write Memory, Authenticated Write Memory, Write Page Protection, and Authenticated Write Page Protection sequence. The interval ends once the device's self-timed EEPROM programming cycle is complete and the current drawn by the device has returned from I_{PROG} to I_{L} .
- Note 20:** The t_{PRS} interval begins immediately after the trailing rising edge on IO for the last time slot of the release byte for a valid Load and Lock Secret sequence, and immediately after the second t_{CSHA} for a valid Compute and Lock Secret sequence. The interval ends once the device's self-timed EEPROM programming cycle is complete and the current drawn by the device has returned from I_{PROG} to I_{L} .
- 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.

DS28EL22

DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM

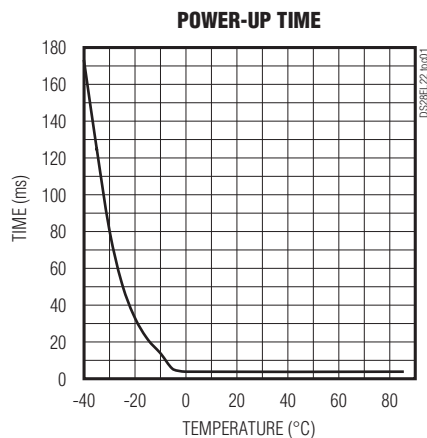
ELECTRICAL CHARACTERISTICS (continued)

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

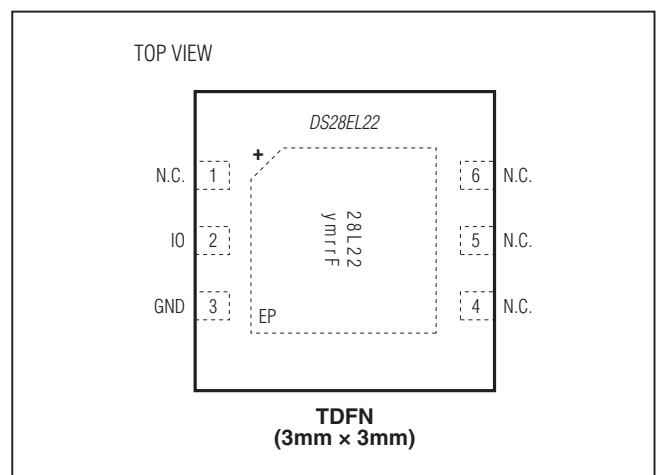
Note 26: The t_{CSHA} interval begins immediately after the trailing rising edge on IO for the last time slot of the release byte for a valid Compute and Lock Secret sequence, immediately after the trailing rising edge on IO for the last time slot of the first cyclic redundancy check (CRC-16) of a Compute and Read Page MAC sequence, immediately after the trailing rising edge on IO for the last time slot of the second CRC-16 byte of an Authenticated Write Memory sequence, immediately after the trailing rising edge on IO for the last time slot of the CRC-16 of an Authenticated Write Page Protection sequence. The interval ends once the device's self-timed SHA-256 computation cycle is complete and the current drawn by the device has returned from I_{CSHA} to I_L .

Typical Operating Characteristics

($V_{\text{PUP}} = 1.71\text{V}$, $V_{\text{IL}} = 0.3\text{V}$, unless otherwise noted.)



Pin Configuration



Pin Description

PIN	NAME	FUNCTION
1, 4, 5, 6	N.C.	Not Connected
2	IO	1-Wire Bus Interface. Open-drain signal that requires an external pullup resistor.
3	GND	Ground Reference
—	EP	Exposed Pad. 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.

ABRIDGED DATA SHEET

DS28EL22

DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb 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/DS28EL22 and click on **Request Full Data Sheet**.

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28EL22Q+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. 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.
6 TDFN-EP	T633+2	21-0137	90-0058