ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

DS28E35

DeepCover Secure Authenticator with 1-Wire ECDSA and 1Kb 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 (DS28E35) provides a highly secure solution for a host controller to authenticate peripherals based on the industry standard (FIPS 186) public-key based Elliptic Curve Digital Signature Algorithm (ECDSA). The ECDSA engine computes keys and signatures using a pseudorandom curve over a prime field according to the "Standards for Efficient Cryptography (SEC)". The private and public key can be computed by the device or installed by the user and optionally locked. Separate memory space is set aside to store and lock a public-key certificate as it is needed to verify authenticity. In addition to ECDSA-related memory, the device has 1024 bits of user memory that is organized as four pages of 256 bits. Page protection modes include write protection, read protection, and one-time-programmable (OTP) memory emulation modes. The DS28E35 also features a one-time settable, nonvolatile 17-bit decrement-on-command counter, which can be used to keep track of the lifetime of the object to which the DS28E35 is attached. 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. The DS28E35 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 multi-device 1-Wire network.

Applications

- Authentication of Consumables
- Peripheral Authentication
- Medical Sensors
- Printer Cartridge Identification and Authentication

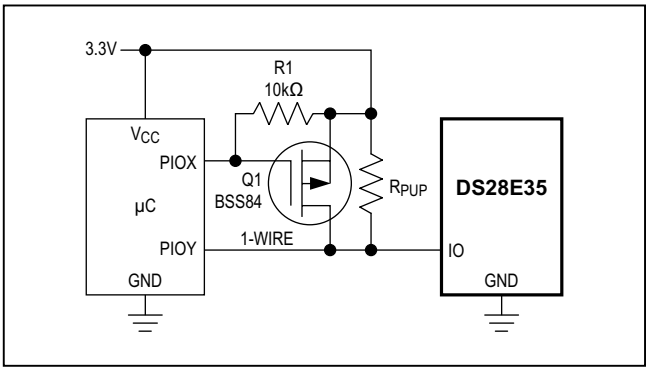
***Ordering Information* appears at end of data sheet.**

For related parts and recommended products to use with this part, refer to www.maximintegrated.com/DS28E35.related.

Features

- ECDSA Engine for Public-Key Signature Using a Defined SEC Domain Parameter Set
- On-Chip Hardware Random Number Generator
- Private and Public Key Can Be Computed by the Device or Loaded from Outside with Optional Automatic Locking
- Separate User-Programmable and Lockable Memory Space to Store a Public-Key Certificate
- 17-Bit One-Time Settable, Nonvolatile Decrement-On-Command Counter
- SHA-256 Engine to Compute a Hash of EEPROM Page Data and Host Challenge for Subsequent ECDSA Signing
- 1024 Bit of User EEPROM Organized as Four Pages of 256 Bits
- Programmable and Irreversible User EEPROM Protection Modes Including Write Protection, Read Protection, and OTP/EPROM Emulation for Individual Memory Pages
- 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%, -40ºC to +85ºC
- ±8kV HBM ESD Protection (typ) for IO Pin
- 8-Pin TDFN and 6-Pin TSOC Packages

Typical Application Circuit



219-0028; Rev 4; 4/14

DS28E35

DeepCover Secure Authenticator with 1-Wire ECDSA and 1Kb User EEPROM

Absolute Maximum Ratings

IO Voltage Range to GND.....-0.5V to +4.0V
IO Sink Current.....20mA
Operating Temperature Range.....-40ºC to +85ºC
Junction Temperature.....+150ºC
Storage Temperature Range.....-55ºC to +125ºC
Lead Temperature (soldering, 10s).....+300ºC
Soldering Temperature (reflow).....+260ºC

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)

TSOC
Junction-to-Ambient Thermal Resistance (θ_{JA}).....126.7°C/W
Junction-to-Case Thermal Resistance (θ_{JC}).....37°C/W

TDFN
Junction-to-Ambient Thermal Resistance (θ_{JA}).....60°C/W
Junction-to-Case Thermal Resistance (θ_{JC}).....11°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 = -40ºC to +85ºC.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V_{PUP}	(Note 3)	2.97		3.63	V
1-Wire Pullup Resistance	R_{PUP}	V_{PUP} = 3.3V ±10% (Note 4)	300		1500	Ω
Input Capacitance	C_{IO}	(Notes 5, 6)		1500		pF
Input Load Current	I_L	IO pin at V_{PUP}		5	50	µA
High-to-Low Switching Threshold	V_{TL}	(Notes 6, 7, 8)		0.65 x V_{PUP}		V
Input Low Voltage	V_{IL}	(Notes 3, 9)			0.3	V
Low-to-High Switching Threshold	V_{TH}	(Notes 6, 7, 10)		0.75 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(Notes 6, 7, 11)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (Note 12)			0.4	V
Recovery Time	t_{REC}	R_{PUP} = 1500Ω (Notes 3, 13)	5			µs
Time Slot Duration	t_{SLOT}	(Notes 3, 14)	13			µs
IO PIN: 1-Wire RESET, PRESENCE DETECT CYCLE						
Reset Low Time	t_{RSTL}	(Note 3)	48		80	µs
Reset High Time	t_{RSTH}	(Note 15)	48			µs
Presence Detect Sample Time	t_{MSP}	(Notes 3, 16)	8		10	µs
IO PIN: 1-Wire WRITE						
Write-Zero Low Time	t_{W0L}	(Notes 3, 17)	8		16	µs
Write-One Low Time	t_{W1L}	(Notes 3, 17)	1		2	µs
IO PIN: 1-Wire READ						
Read Low Time	t_{RL}	(Notes 3, 18)	1		2 - δ	µs
Read Sample Time	t_{MSR}	(Notes 3, 18)	t_{RL} + δ		2	µs

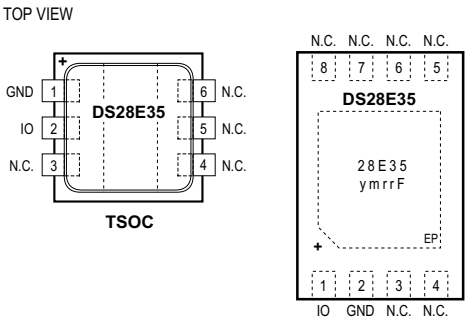
Electrical Characteristics (continued)

(T_A = -40ºC to +85ºC.) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX
EEPROM					
Programming Current	I_{PROG}	V_{PUP} = 3.63V (Notes 6, 19)		1	mA
Programming Time Unit	t_{PROG}	**Refer to the full data sheet.**			ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85ºC (Notes 21, 22)	100k		—
Data Retention	t_{DR}	T_A = +85ºC (Notes 23, 24, 25)	10		years
ECDSA ENGINE					
Computation Current	I_{ECE}	**Refer to the full data sheet.**			mA
Key Pair Computation Time	t_{GKP}				ms
Signature Computation Time	t_{GPS}				ms

Note 2: Limits are 100% production tested at T_A = +25ºC and T_A = +85ºC. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are at T_A = +25ºC.
Note 3: System requirement.
Note 4: 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 5: 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 6: Guaranteed by design and/or characterization only; not production tested.
Note 7: 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 8: Voltage below which, during a falling edge on IO, a logic-zero is detected.
Note 9: The voltage on IO must be less than or equal to V_{ILMAX} at all times the master is driving IO to a logic-zero level.
Note 10: Voltage above which, during a rising edge on IO, a logic-one is detected.
Note 11: 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 12: The I-V characteristic is linear for voltages less than 1V.
Note 13: Applies to a single device attached to a 1-Wire line. 100% production tested at T_A = +85ºC, +25ºC, and -40ºC.
Note 14: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.
Note 15: An additional reset or communication sequence cannot begin until the reset high time has expired.
Note 16: Interval after t_{RSTL} during which a bus master can read a logic-zero on IO if there is a DS28E35 present. The power-up presence detect pulse could be outside this interval, but is complete within 2ms after power-up.
Note 17: 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 $t_{W1LMAX} + t_F - \varepsilon$ and $t_{W0LMAX} + t_F - \varepsilon$, respectively.
Note 18: 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 $t_{RLMAX} + t_F$.
Note 19: Current drawn from IO during the EEPROM programming interval. The pullup circuit on IO during the programming interval should be such that the voltage at IO is greater than or equal to 2.5V.
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.**
Note 27: **Refer to the full data sheet.**
Note 28: **Refer to the full data sheet.**

Pin Configuration



PACKAGE SIZES NOT DRAWN TO SCALE

Pin Description

PIN		NAME	FUNCTION
TSOC	TDFN-EP		
1	2	GND	Ground Reference
2	1	IO	1-Wire Bus Interface. Open-drain signal that requires an external pullup resistor.
3–6	3–8	N.C.	Not Connected
—	EP	EP	Exposed Pad. Solder evenly to the board's ground plane for proper operation. Refer to Application Note 3273: Exposed Pads: *A Brief Introduction* for additional information.

ABRIDGED DATA SHEET

DS28E35

DeepCover Secure Authenticator with 1-Wire ECDSA and 1Kb User EEPROM

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28E35Q+T**	-40ºC to +85ºC	8 TDFN-EP* (2.5k pcs)
DS28E35P+	-40ºC to +85ºC	6 TSOC
DS28E35P+T	-40ºC to +85ºC	6 TSOC (4k pcs)

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

T = Tape and reel.

**EP = Exposed pad.*

***Future product—contact factory for availability.*

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 TSOC	D6+1	21-0382	90-0321
8 TDFN-EP	T823+1	21-0174	90-0091

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/DS28E35** and click on **Request Full Data Sheet**.