Request Security User Guide and Developer Software ›

EVALUATION KIT AVAILABLE

*Click **here** for production status of specific part numbers.*

DS28C39

DeepCover Secure ECDSA Bidirectional Authenticator with ChipDNA PUF Protection

General Description

The DS28C39 is an ECDSA public-key-based bidirectional secure authenticator that incorporates Maxim's patented ChipDNA™ feature, a physically unclonable function (PUF) to provide a cost-effective solution with the ultimate protection against security attacks. Using the random variation of semiconductor device characteristics that naturally occur during wafer fabrication, the ChipDNA circuit generates a unique output value that is repeatable over time, temperature, and operating voltage. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, preventing discovery of the unique value used by the chip cryptographic functions. The DS28C39 utilizes the ChipDNA output as key content to cryptographically secure all device stored data and as the private key for the ECDSA signing operation. With ChipDNA capability, the device provides a core set of cryptographic tools derived from integrated blocks including an asymmetric (ECC-P256) hardware engine, a FIPS/NIST-compliant true random number generator (TRNG), 2Kb of secured EEPROM, a decrement-only counter and a unique 64-bit ROM identification number (ROM ID). The ECC public/ private key capabilities operate from the NIST-defined P-256 curve to provide a FIPS 186-compliant ECDSA signature generation function. The unique ROM ID is used as a fundamental input parameter for cryptographic operations and serves as an electronic serial number within the application. Lastly, the DS28C39 supports I^{2}C communication at the 100kHz standard mode.

Applications

- Authentication of Medical Sensors and Tools
- Secure Management of Limited Use Consumables
- IoT Node Authentication
- Peripheral Authentication
- Reference Design License Management
- Printer Cartridge Identification and Authentication

Benefits and Features

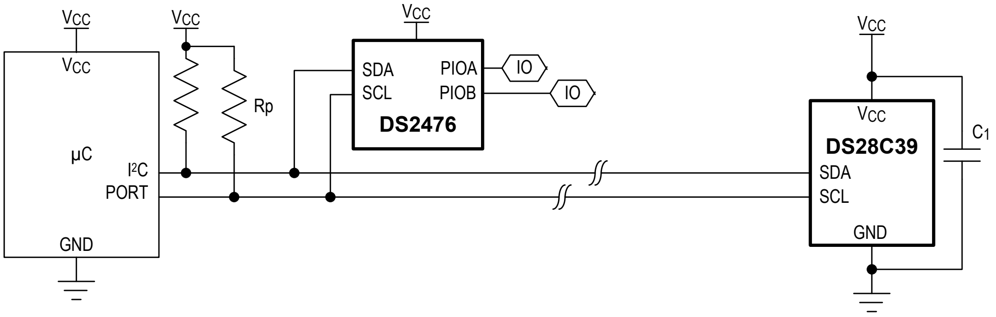
- Robust Countermeasures Protect Against Security Attacks
  - Patented Physically Unclonable Function Secures Device Data
  - Actively Monitored Die Shield Detects and Reacts to Intrusion Attempts
  - All Stored Data Cryptographically Protected from Discovery
- ECDSA Authenticated R/W of Stored Data and Counter
- Efficient Public-Key Authentication Solution to Authenticate Peripherals
  - FIPS 186-Compliant ECDSA P256 Signature for Challenge/Response Authentication
  - ChipDNA Generated Public/Private Key Pair.
  - TRNG with NIST SP 800-90B Compliant Entropy Source
- Supplemental Features Enable Easy Integration into End Applications
  - 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
  - 2Kb of EEPROM for User Data, Key, Control Registers, and Certificate
  - Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - I^{2}C Communication: Up to 200kHz
  - Operating Range: 3.3V ±10%, -40°C to +85°C
  - 6-Pin TDFN-EP Package (3mm x 3mm)

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

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

maxim integrated™

Typical Application Circuit



Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND	-0.5V to 4.0V
Maximum Current into Any Pin	-20mA to 20mA
Operating Temperature Range	-40°C to +85°C
Junction Temperature	+150°C
Storage Temperature Range	-40°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 Information

6 TDFN-EP

Package Code	T633+2
Outline Number	**21-0137**
Land Pattern Number	**90-0058**
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	55°C/W
Junction to Case (θ_{JC})	9°C/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	42°C/W
Junction to Case (θ_{JC})	9°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 = 25ºC. 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. Specifications to the minimum and maximum operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}	(Note 1)	2.97	3.3	3.63	V
Supply Current	I_{CC}	Standby			4	mA
		Communicating/active (Note 2)			10	mA
CRYPTO FUNCTIONS						
Computation Current	I_{CMP}	(Note 3)			10	mA
Generate ECC Key Pair	t_{GKP}				200	ms
Generate ECDSA Signature	t_{GES}				130	ms
TRNG On-Demand Check	t_{ODC}				20	ms
EEPROM						
Read Memory	t_{RM}				30	ms
Write Memory	t_{WM}				65	ms
Write State	t_{WS}				15	ms
Write/Erase Cycles (Endurance)	N_{CY}	T_A = +85°C (Note 4)	100K			
Data Retention	t_{DR}	T_A = +85°C (Note 5)	10			years
I²C SCL AND SDA PINS (Note 6)						
Low-Level Input Voltage	V_{IL}		-0.3		0.3 × V_{CC}	V
High-Level Input Voltage	V_{IH}		0.85 × V_{CC}		V_{CC} + 0.3V	V
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 2)		0.1 × V_{CC}		V
Low-Level Output Voltage at 4mA Sink Current	V_{OL}	(Note 7)			0.4	V
Output Fall Time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$ with a Bus Capacitance from 10pF to 400pF	t_{OF}	(Note 2)		180		ns
Input Current with an Input Voltage Between 0.1V_{CCmax} and 0.9V_{CCmax}	I_I	(Note 2)	-1		+1	µA

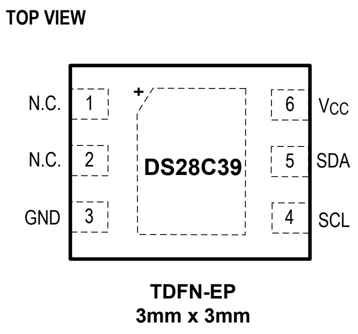
Electrical Characteristics (continued)

(Limits are 100% production tested at T_A = +25°C and/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 not guaranteed.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Input Capacitance	C_I	(Note 2)		10		pF
SCL Clock Frequency	f_{SCL}	(Note 1)	0		200	kHz
Hold Time (Repeated) START Condition	$t_{HD:STA}$		1			µs
Low Period of the SCL Clock	t_{LOW}	(Note 8)	1			µs
High Period of the SCL Clock	t_{HIGH}	(Note 2)	3			µs
Setup Time for a Repeated START Condition	$t_{SU:STA}$	(Note 2)	1			µs
Data Hold Time	$tH_{D:DAT}$	(Notes 2, 8, 9)			0.55	µs
Data Setup Time	$t_{SU:DAT}$	(Notes 2, 8, 10)	250			ns
Setup Time for STOP Condition	$t_{SU:STO}$	(Note 2)	1			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}	(Note 2)	2			µs
Capacitive Load for Each Bus Line	C_B	(Notes 1, 11)			400	pF
Warm-Up Time	t_{OSCWUP}	(Note 1, 12)			12	ms

Note 1: System requirement.
Note 2: Guaranteed by design and/or characterization only. Not production tested.
Note 3: Current drawn from V_{CC} during the EEPROM programming interval or Crypto computation.
Note 4: Write-cycle endurance is tested in compliance with JESD47G.
Note 5: Data retention is tested in compliance with JESD47G.
Note 6: All I^2C timing values are referred to $V_{IH(MIN)}$ and $V_{IL(MAX)}$ levels.
Note 7: The I-V characteristic is linear for voltages less than 1V.
Note 8: t_{LOW} min = $t_{HD:DAT}$ max + 200ns for rise or fall time + $t_{SU:DAT}$ min. Values greater than these can be accommodated by extending t_{LOW} accordingly.
Note 9: The DS28C39 provides a hold time of at least 100ns for the SDA signal (referenced to the $V_{IH(MIN)}$ of the SCL signal) to bridge the undefined region of the falling edge of SCL.
Note 10: The DS28C39 can be used in a standard-mode I^2C-bus system, but the requirement $t_{SU:DAT}$ ≥ 250ns must then be met. Also the acknowledge timing must meet this setup time (I^2C bus specification Rev. 03, 19 June 2007).
Note 11: C_B = Total capacitance of one bus line in pF. The maximum bus capacitance allowable may vary from this value depending on the actual operating voltage and frequency of the application (I^2C bus specification Rev. 03, 19 June 2007).
Note 12: I^2C communication should not take place for the max t_{OSCWUP} time following a power-on reset.

Pin Configuration



Pin Description

PIN	NAME	FUNCTION
1, 2	N.C.	No Connection. The pins are not wire-bonded to the IC pads.
3	GND	Ground
4	SCL	I^2C Serial Clock Input. Must be connected to V_{CC} through a pullup resistor.
5	SDA	Open-Drain, I^2C Serial Data Input/Output. Must be connected to V_{CC} through a pullup resistor.
6	V_{CC}	Power Supply Input
–	EP	Exposed Pad (TDFN Only). Solder evenly to the board's ground plane for proper operation. Refer to Application Note 3273: *Exposed Pads: A Brief Introduction* for additional information.

Detailed Description

The DS28C39 is the first I²C secure authenticator to integrate the Maxim ChipDNA capability to protect all device stored data from invasive discovery. The ChipDNA output is used as the ECC-P256 private key. In addition to the ChipDNA circuit and ECC-P256 engines for signatures, the device integrates a FIPS/NIST-compliant TRNG, 2Kb EEPROM for user memory, ECC key set, control registers, and certificates. One user page can optionally be designated as a decrement-only counter. The device operates from an I²C interface with support for 100kHz. Figure 1 shows the relationships between the circuit elements of the DS28C39.

Design Resource Overview

Operation of the DS28C39 involves use of device EEPROM and execution of device function commands. The following provides an overview including the decrement counter. Refer to the *DS28C39 Security User Guide* for details.

Memory

A 2Kb secured EEPROM array provides storage options for an ECDSA key pair and certificate, 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.

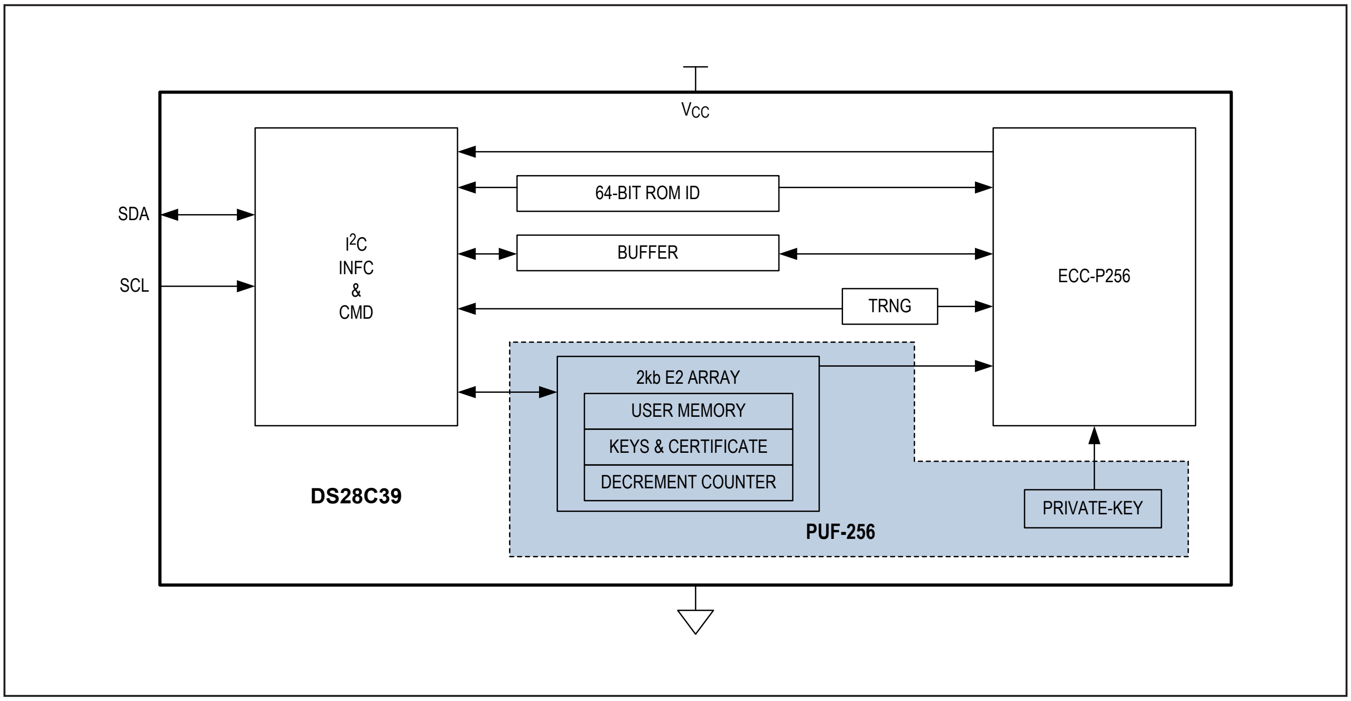


Figure 1. Block Diagram

I^2C

General Characteristics

The I^2C bus uses a data line (SDA) plus a clock signal (SCL) for communication. Both SDA and SCL are bidirectional lines, connected to a positive supply voltage through a pullup resistor. When there is no communication, both lines are high. The output stages of devices connected to the bus must have an open drain or open collector to perform the wired-AND function. Data on the I^2C bus can be transferred at rates of up to 100kbps. A device that sends data on the bus is defined as a transmitter, and a device receiving data is defined as a receiver. The device that controls the communication is called a master. The devices that are controlled by the master are slaves. To be individually accessed, each device must have a slave address that does not conflict with other devices on the bus. Data transfers can be initiated only when the bus is not busy. The master generates the serial clock (SCL), controls the bus access, generates the START and STOP conditions, and determines the number of data bytes transferred between START and STOP Figure 2. Data is transferred in bytes with the most significant bit being transmitted first. After each byte follows an acknowledge bit to allow synchronization between master and slave.

Slave Address

The slave address to which the DS28C39 responds is shown in Figure 3. The slave address is part of the slave address/control byte. The last bit of the slave address/control byte (R/W) defines the data direction. When set to 0, subsequent data flows from master to slave (write access); when set to 1, data flows from slave to master (read access).

I^2C Definitions

The following terminology is commonly used to describe I^2C data transfers. The timing references are defined in Figure 4.

Bus Idle or Not Busy

Both SDA and SCL are inactive and in their logic-high states.

START Condition

To initiate communication with a slave, the master must generate a START condition. A START condition is defined as a change in state of SDA from high to low while SCL remains high.

STOP Condition

To end communication with a slave, the master must generate a STOP condition. A STOP condition is defined as a change in state of SDA from low to high while SCL remains high.

Repeated START Condition

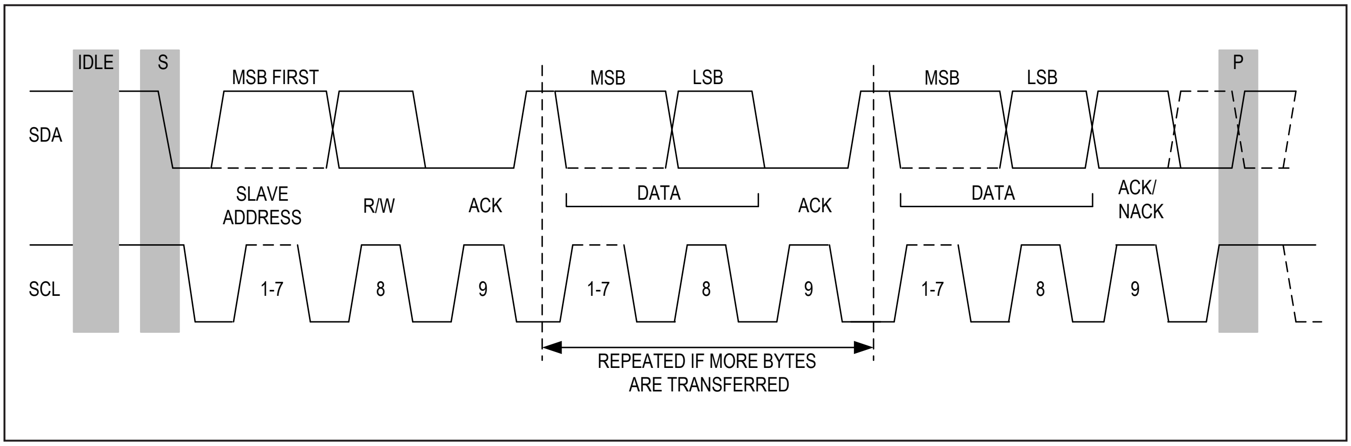


Figure 2. I^2C Protocol Overview

Repeated STARTs are commonly used for read accesses after having specified a memory address to read from in a preceding write access. The master can use a repeated START condition at the end of a data transfer to immediately initiate a new data transfer following the current one. A repeated START condition is generated the same way as a normal START condition, but without leaving the bus idle after a STOP condition.

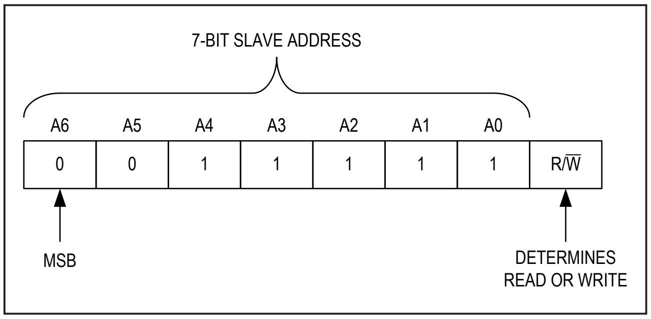
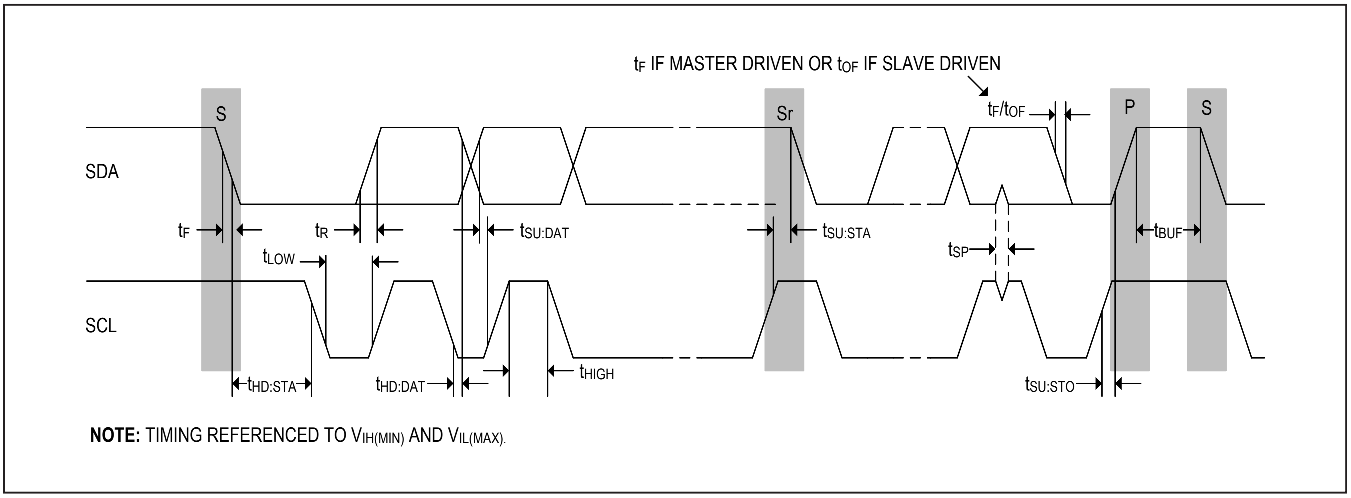


Figure 3. DS28C39 I²C Slave Address

Data Valid

With the exception of the START and STOP condition, transitions of SDA can occur only during the low state of SCL. The data on SDA must remain valid and unchanged during the entire high pulse of SCL plus the required setup and hold time ($t_{HD:DAT}$ after the falling edge of SCL and $t_{SU:DAT}$ before the rising edge of SCL; see Figure 4). There is one clock pulse per bit of data. Data is shifted into the receiving device during the rising edge of the SCL pulse.

When finished with writing, the master must release the SDA line for a sufficient amount of setup time (minimum $t_{SU:DAT,}$ + t_R in Figure 4) before the next rising edge of SCL to start reading. The slave shifts out each data bit on SDA at the falling edge of the previous SCL pulse and the data bit is valid at the rising edge of the current SCL pulse. The master generates all SCL clock pulses, including those needed to read from a slave.



NOTE: TIMING REFERENCED TO $V_{IH(MIN)}$ AND $V_{IL(MAX)}$.

Figure 4. I²C Timing Diagram

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28C39Q+T	-40°C to +85°C	6 TDFN (2.5k pcs)

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

T = Tape and reel.