DS28C16

I²C Low-Voltage SHA-3 Authenticator

General Description

The DS28C16 secure authenticator combines FIPS202-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.

Applications

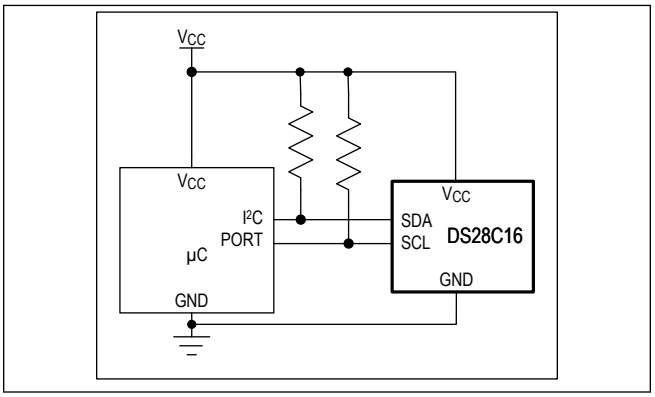
- Medical Tools/Accessories Authentication and Calibration
- Accessory and Peripheral Secure Authentication
- Battery Authentication and Charge Cycle Tracking

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
  - Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - I²C Communications Up to 1MHz
  - Operating Range: 1.62V–3.63V, -40°C to +85°C
  - 8-Pin, 2mm x 2mm TDFN-EP Package

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

Typical Application Circuit



19-100753; Rev 0; 3/20

maxim integrated™

TABLE OF CONTENTS

General Description . . . 1
Applications . . . 1
Benefits and Features . . . 1
Typical Application Circuit . . . 1
Absolute Maximum Ratings . . . 4
Package Information . . . 4
8 TDFN-EP . . . 4
Electrical Characteristics . . . 4
Pin Configuration . . . 6
TDFN . . . 6
Pin Description . . . 7
Detailed Description . . . 8
Design Resource Overview . . . 8
Memory . . . 8
Decrement Counter . . . 8
I²C . . . 8
General Characteristics . . . 8
Slave Address . . . 9
I²C Definitions . . . 9
Bus Idle or Not Busy . . . 9
START Condition . . . 10
STOP Condition . . . 10
Repeated START Condition . . . 10
Data Valid . . . 10
Ordering Information . . . 11
Revision History . . . 12

LIST OF FIGURES

Figure 1. Block Diagram 8
Figure 2. I²C Protocol Overview 9
Figure 3. I²C Slave Address 9
Figure 4. I²C Timing Diagram 10

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

8 TDFN-EP

Package Code	T822+3C
Outline Number	21-0168
Land Pattern Number	90-0065
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	—
Junction to Case (θ_{JC})	—
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	85.1°C/W
Junction to Case (θ_{JC})	20.8°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 and T_A = +85ºC. 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 operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}	(*Note 1*)	1.62	3.3	3.63	V
Supply Current	I_{CC}	Standby		3.5	12	µA
		Communicating (*Note 2*)			60	
I²C SCL AND SDA PINS (*Note 3*)						
Low-Level Input Voltage	V_{IL}		-0.3		0.3 × V_{CC}	V
High-Level Input Voltage	V_{IH}	V_{CC} > 1.98V	0.7 × V_{CC}		V_{CC} + 0.3	V
		V_{CC} ≤ 1.98V	0.8 × V_{CC}		V_{CC} + 0.3	
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(*Note 4*)		0.05 × V_{CC}		V
Low-Level Output Voltage at 4mA Sink Current	V_{OL}	(*Note 5*)			0.4	V

Electrical Characteristics (continued)

(Limits are 100% 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. Specifications marked GBD are guaranteed by design and not production tested. Specifications to the minimum operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Output Fall Time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$ with a Bus Capacitance from 10pF to 400pF	t_{OF}	(*Note 4*)		30		ns
Pulse Width of Spikes that are Suppressed by the Input Filter	t_{SP}				50	ns
Input Current with an Input Voltage Between $0.1V_{CCmax}$ and $0.9V_{CCmax}$	I_I	(*Note 4*, *Note 6*)	-1		+1	µA
Input Capacitance	C_I	(*Note 4*)		10		pF
SCL Clock Frequency	f_{SCL}	(*Note 1*)			1	MHz
Hold Time (Repeated) START Condition	$t_{HD:STA}$		0.45			µs
Low Period of the SCL Clock	t_{LOW}	(*Note 7*)	0.65			µs
High Period of the SCL Clock	t_{HIGH}		0.35			µs
Setup Time for a Repeated START Condition	$t_{SU:STA}$		0.35			µs
Data Hold Time	$t_{HD:DAT}$	(*Note 4*, *Note 7*, *Note 8*)			0.35	µs
Data Setup Time	$t_{SU:DAT}$	(*Note 7*, *Note 9*)	100			ns
Setup Time for STOP Condition	$t_{SU:STO}$		0.35			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}		0.6			µs
Capacitive Load for Each Bus Line	C_B	(*Note 1*, *Note 10*)			400	pF
Warm-Up Time	t_{OSCWUP}	(*Note 1*, *Note 11*)			1	ms
CRYPTO FUNCTIONS						
Computation Current	I_{CMP}				3	mA
Read Memory Time	t_{RM}				5	ms
Write Memory Time	t_{WM}				60	ms
Short Write Memory Time	t_{WMS}				15	ms
Computation Time	t_{CMP}				15	ms
EEPROM						
Write/Erase Cycles (Endurance)	N_{CY}	(*Note 12*)	100K			

Electrical Characteristics (continued)

(Limits are 100% 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. Specifications marked GBD are guaranteed by design and not production tested. Specifications to the minimum operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Data Retention	t_{DR}	T_A = +85ºC (*Note 13*)	10			years

Note 1: System requirement.

Note 2: Operating current during I²C communication at 1MHz with < 25ns rise and fall times on SDA and SCL.

Note 3: All I²C timing values are referred to $V_{IH(MIN)}$ and $V_{IL(MAX)}$ levels.

Note 4: Guaranteed by design and/or characterization only. Not production tested.

Note 5: The I-V characteristic is linear for voltages less than 1V.

Note 6: I/O pins of the DS28C16 do not obstruct the SDA and SCL lines if V_{CC} is switched off.

Note 7: 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 8: The DS28C16 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 9: The DS28C16 can be used in a standard-mode I²C-bus system, but the requirement $t_{SU:DAT} \geq 250$ns must then be met. Also, the acknowledge timing must meet this setup time (I²C bus specification Rev. 03, 19 June 2007).

Note 10: 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 (I²C bus specification Rev. 03, 19 June 2007).

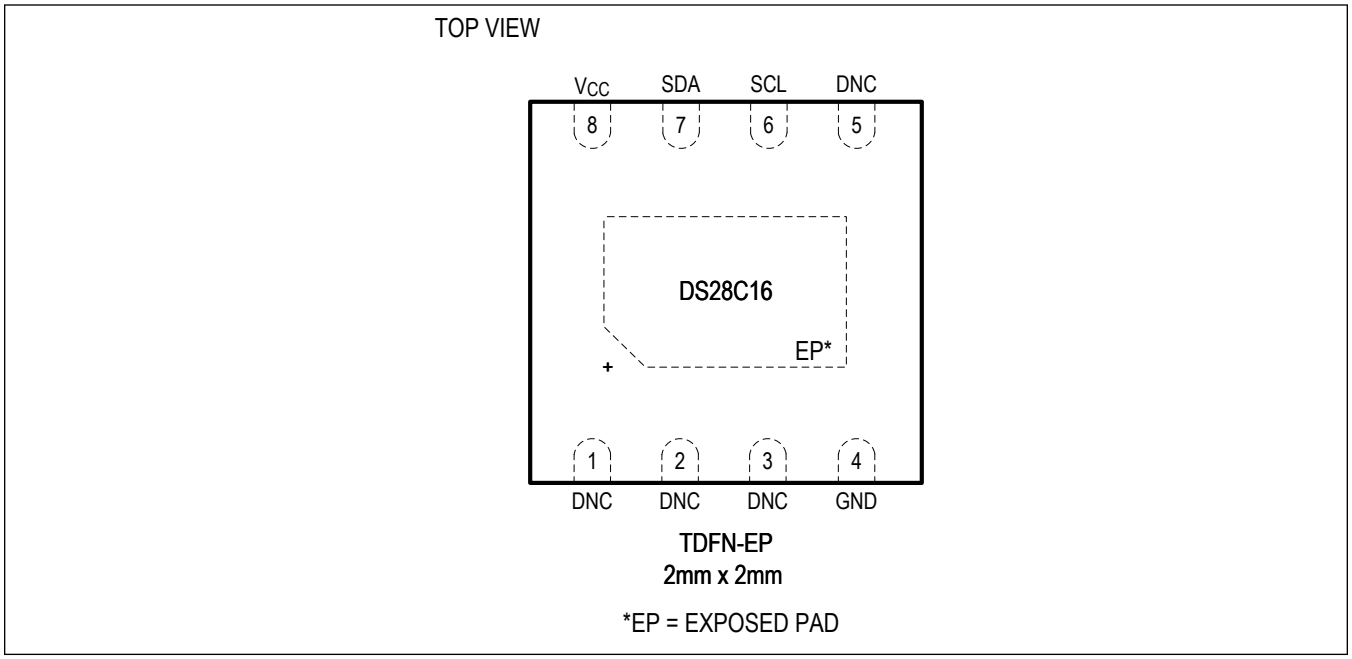
Note 11: I²C communication should not take place for at least t_{OSCWUP} after V_{CC} reaches $V_{CC(MIN)}$.

Note 12: Write-cycle endurance is tested in compliance with JESD47H.

Note 13: Data retention is tested in compliance with JESD47H.

Pin Configuration

TDFN



TDFN-EP
2mm x 2mm

*EP = EXPOSED PAD

Pin Description

PIN	NAME	FUNCTION
1–3, 5	DNC	Do Not Connect
4	GND	Ground Reference. Connect all contacts to GND.
6	SCL	I²C Clock. Connect to V_{CC} with pullup resistor.
7	SDA	I²C Data. Connect to V_{CC} with pullup resistor.
8	V_{CC}	Supply Voltage
—	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 DS28C16 integrates the Maxim DeepCover® capability to protect all device stored data from invasive discovery. In addition to the SHA-3 engine for signatures, 256-bit EEPROM for user memory, SHA-3 secret storage, 17-bit decrement counter, and control registers. The device operates from an I²C interface.

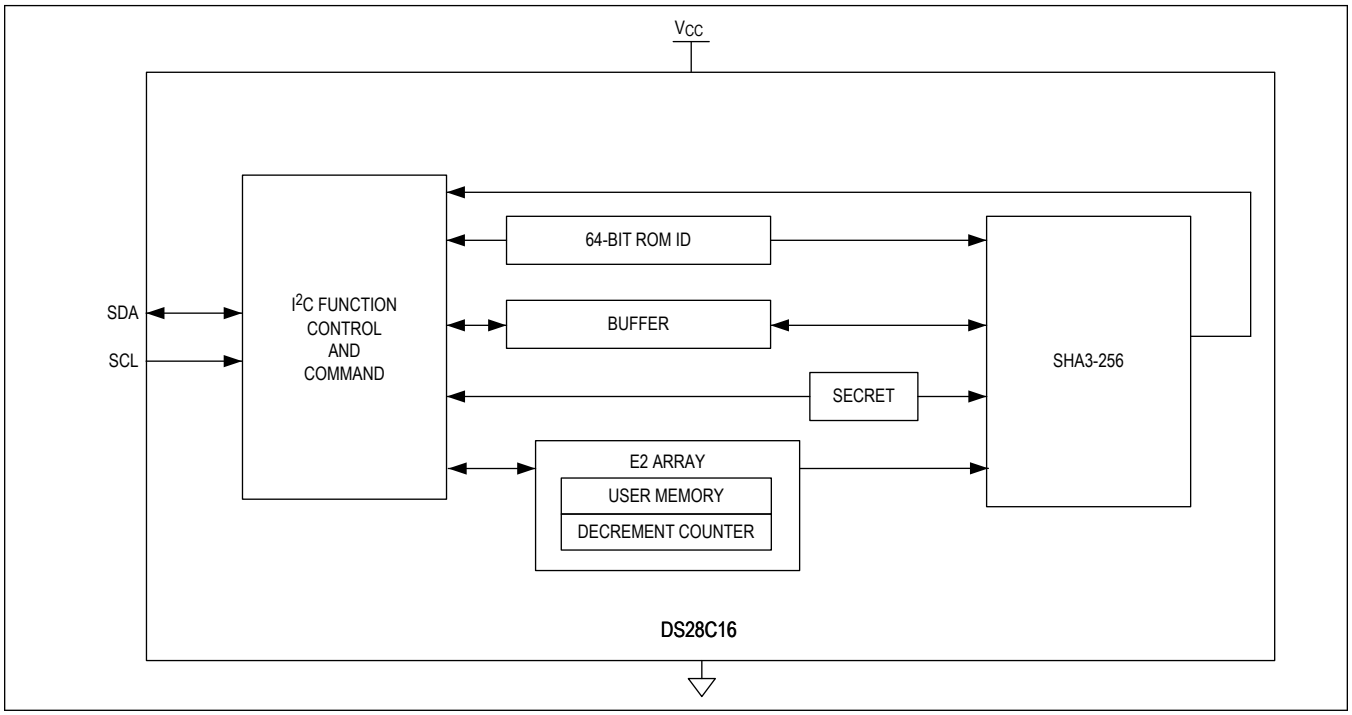


Figure 1. Block Diagram

Design Resource Overview

Operation of the DS28C16 involves use of device EEPROM and execution of device function commands. The following section provides an overview including the decrement counter. Refer to the *DS28C16 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.

I²C

General Characteristics

The I²C 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 I²C bus can be transferred at rates up to 100kbps in standard mode and up to 400kbps in fast mode. The DS28C16 works in both modes or up to a clock rate of 1MHz. 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 communication is called a master. Devices 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. An acknowledge bit follows each byte to allow synchronization between master and slave.

Slave Address

The slave address to which the DS28C16 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).

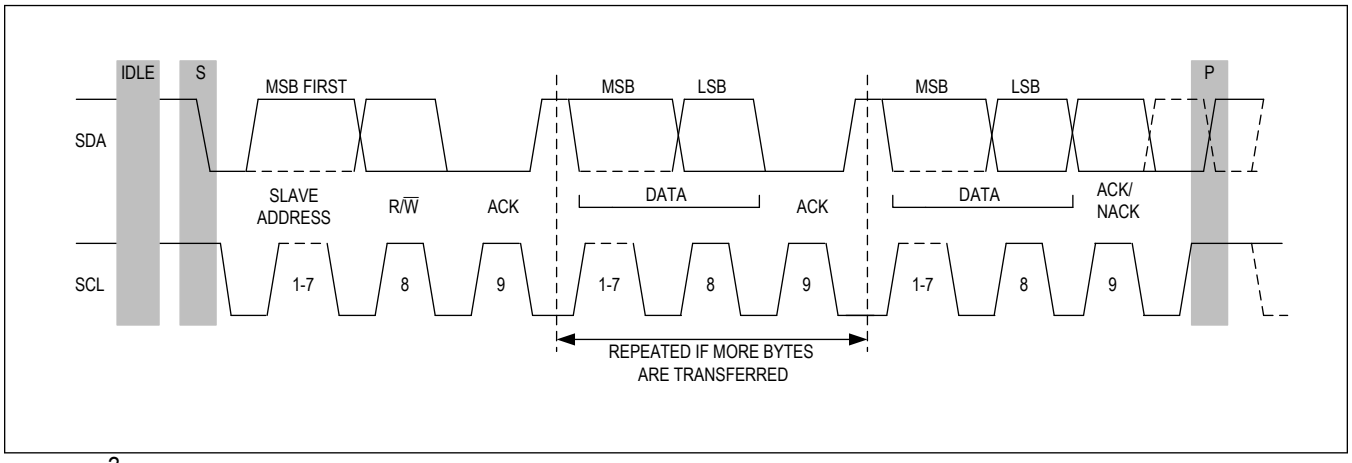


Figure 2. I²C Protocol Overview

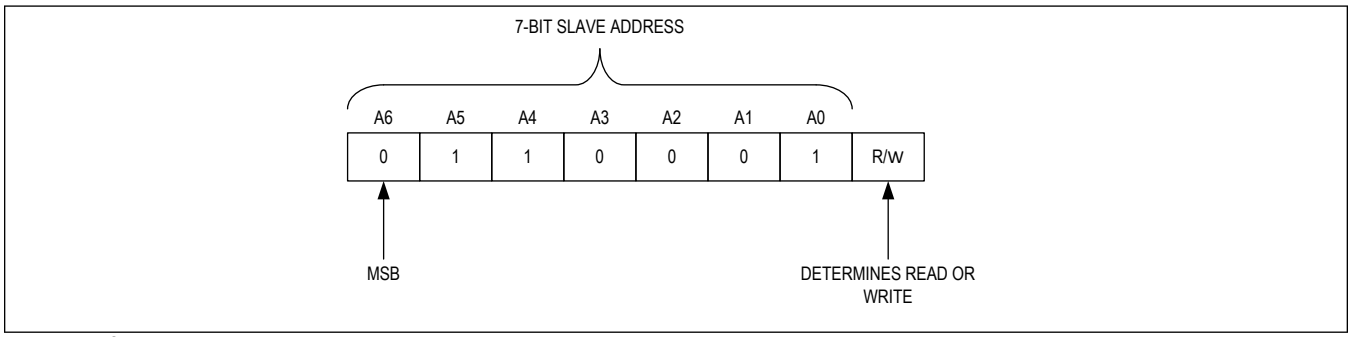


Figure 3. I²C Slave Address

I²C Definitions

The following terminology is commonly used to describe I²C 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

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.

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.

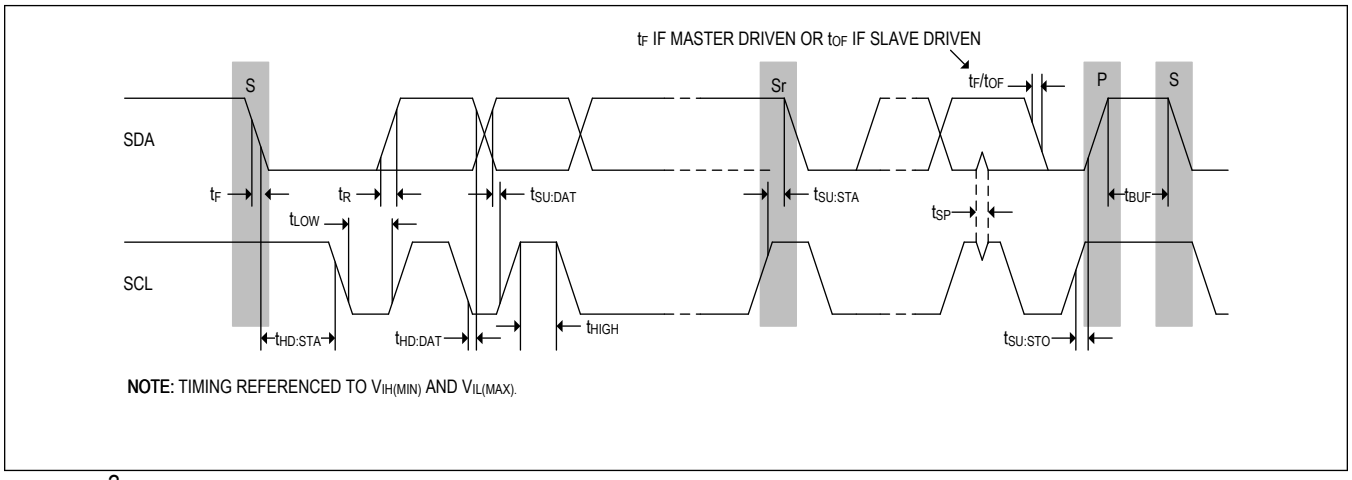


Figure 4. I²C Timing Diagram

Ordering Information

PART NUMBER	TEMP RANGE	PIN-PACKAGE
DS28C16Q+T	-40°C to +85°C	8 TDFN-EP* (2.5k pcs)

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

T = Tape and reel.

**EP = Exposed pad.*

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	3/20	Initial release	—

For pricing, delivery, and ordering information, please visit Maxim Integrated's online storefront at https://www.maximintegrated.com/en/storefront/storefront.html.

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.

Maxim Integrated and the Maxim Integrated logo are trademarks of Maxim Integrated Products, Inc. © 2020 Maxim Integrated Products, Inc.