*Click **here** to ask an associate for production status of specific part numbers.*

DS2478

DeepCover Automotive Secure Coprocessor

General Description

The DS2478 is a DeepCover® secure ECDSA and HMAC SHA-256 coprocessor companion to the DS28E40 or DS28C40. The coprocessor can compute any required HMACs or ECDSA signatures to do any operation on the DS28E40 or DS28C40. The DS2478 provides a core set of cryptographic tools derived from integrated asymmetric (ECC P-256) and symmetric (SHA-256) security functions. In addition to the security services provided by the hardware implemented crypto engines, the device integrates a FIPS/NIST true random number generator (TRNG), 6Kb of secured one-time-programmable (OTP) memory, one configurable GPIO, and a unique 64-bit ROM identification number (ROM ID).

The ECC public/private key capabilities operate from the NIST-defined P-256 curve and include FIPS 186-compliant ECDSA signature generation and verification to support a bidirectional asymmetric key authentication model. The SHA-256 secret-key capabilities are compliant with FIPS 180 and are flexibly used in conjunction with ECDSA operations or independently for multiple HMAC functions.

The GPIO pin can be operated under command control and include configurability supporting authenticated and nonauthenticated operation including an ECDSA-based crypto-robust mode to support secure-boot of a host processor. This secure-boot method can also be used to enable the coprocessor functions.

DeepCover embedded security solutions cloak sensitive data under multiple layers of advanced security to provide the most secure key storage possible. To protect against device-level security attacks, invasive and noninvasive countermeasures are implemented, including an active die shield, encrypted storage of keys, and algorithmic methods.

Applications

- Automotive Secure Authentication
- Identification and Calibration Automotive of Parts/Tools/Accessories
- IoT Node Crypto-Protection
- Secure Authentication of Accessories and Peripherals
- Secure Storage of Cryptographic Keys for a Host Controller
- Secure Boot or Download of Firmware and/or System Parameters

Benefits and Features

- HW Accelerator Offloads ECDSA and SHA-256 Computations from Host Processor
  - FIPS 186 ECDSA P-256 Signature and Verification
  - ECDH Key Exchange for Session Key Establishment
  - ECDSA-Authenticated R/W of Configurable Memory
  - FIPS 180 HMAC for Bidirectional Authentication
- SHA-256 One-Time Pad Encrypted R/W of Configurable Memory Using an ECDH Established Key
- One GPIO Pin with Optional Authentication Control
  - Open Drain, 4mA/0.4V
  - Optional SHA-256 or ECDSA-Authenticated On/Off and State Read
  - Optional ECDSA Certificate to Set On/Off after Multiblock Hash for Secure Boot
- TRNG with NIST SP 800-90B Compliant Entropy Source with Function to Read Out
- Optional Chip-Generated Pr/Pu Key Pairs for ECC Operations
- 6Kb of One-Time Programmable (OTP) Memory for User Data, Keys, and Certificates
- Unique and Unalterable, Factory-Programmed, 64-Bit Identification Number (ROM ID)
  - Optional Input Data Component to Crypto and Key Operations
- I^2C Communication up to 1MHz
- 3.3V ±10%, -40°C to +125°C Operating Range
- 10-Pin, 3mm x 3mm, Side-Wettable TDFN Package
- AEC-Q100 Grade 1

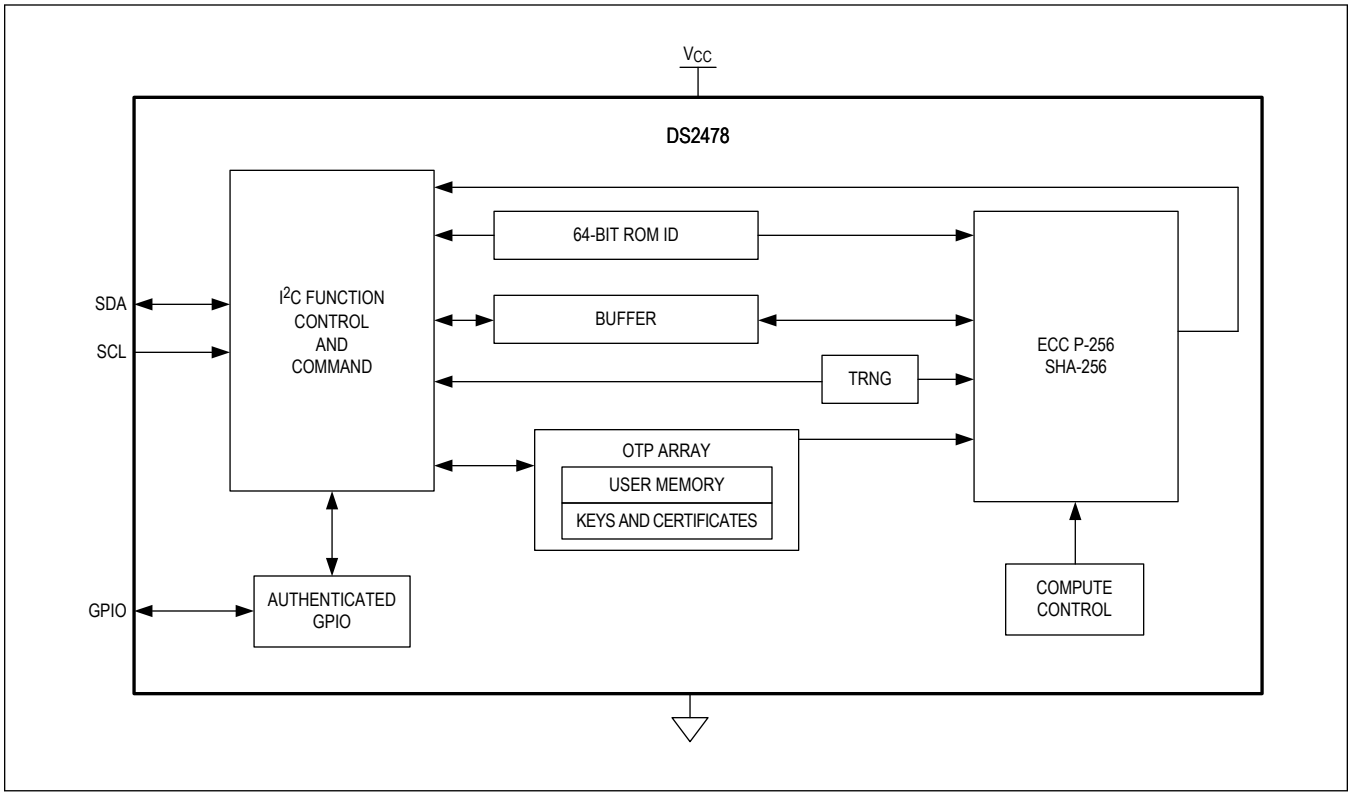
Request DS2478 Security User Guide

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

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

19-101425; Rev 0; 1/22

Simplified Block Diagram



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 +125°C
Junction Temperature ..... +150°C
Storage Temperature Range .....-40°C to +150°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

10 TDFN (3mm x 3mm)

Package Code	T1033Y+2
Outline Number	21-100346
Land Pattern Number	90-0003
Thermal Resistance, Four-Layer Board	
Junction to Ambient (θ_{JA})	39.71°C/W
Junction to Case (θ_{JC})	2.73°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 = +25°C. 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		0.5	2	mA
		Communicating (*Note 2*)			16.5	
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}		0.7 × V_{CC}		V_{CC} + 0.3	V
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
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

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25°C. 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
Pulse Width of Spikes Suppressed by the Input Filter	t_{SP}	(*Note 4*)			50	ns
Input Current with an Input Voltage between $0.1V_{CC\_MAX}$ and $0.9V_{CC\_MAX}$	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}	(*Note 4*)	0.35			µs
Setup Time for a Repeated START Condition	$t_{SU:STA}$	(*Note 4*)	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 4*, *Note 7*, *Note 9*)	100			ns
Setup Time for STOP Condition	$t_{SU:STO}$	(*Note 4*)	0.35			µs
Bus Free Time between a STOP and START Condition	t_{BUF}	(*Note 4*)	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
GPIO PIN						
GPIO Output Low	$PIOV_{OL}$	$PIOI_{OL}$ = 4mA (*Note 5*)			0.4	V
GPIO Input Low	$PIOV_{IL}$		-0.3		0.3 x V_{CC}	V
GPIO Master Sample	$PIOV_{IH}$		0.70 x V_{CC}		V_{CC} + 0.3	V
GPIO Switching Hysteresis	$PIOV_{HY}$			0.3		V
GPIO Leakage Current	$PIOI_L$		-1		+1	µA
CRYPTO FUNCTIONS						
Computation Current	I_{CMP}	(*Note 2*)		11	16.5	mA
Read Memory	t_{RM}				2	ms
Write Memory	t_{WM}				150	ms
Write State	t_{WS}				15	ms

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25°C. 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
Computation Time (HMAC)	t_{CMP}				4	ms
Generate ECC Key Pair	t_{GKP}				500	ms
Generate ECDSA Signature	t_{GES}				50	ms
Verify ECDSA Signature or Compute ECDH Time	t_{VES}				160	ms
TRNG Generation	t_{RNG}				50	ms
TRNG On-Demand Check	t_{ODC}				50	ms
OTP						
OTP Write Temperature	T_{OPTW}		0		50	°C
Data Retention	t_{DR}	T_A = +125°C (*Note 12*)	10			years

Note 1: System requirement.

Note 2: OTP programming current production tested at +25°C.

Note 3: All I^2C 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 DS2478 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 DS2478 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 DS2478 can be used in a standard-mode I^2C-bus system, but the requirement $t_{SU:DAT} \geq 250ns$ must then be met. Also, the acknowledge timing must meet this setup time (I^2C Bus Specification Rev. 03, 19 June 2007).

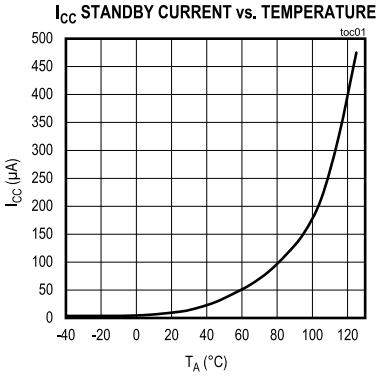
Note 10: C_B = Total capacitance of one bus line in pF. The maximum bus capacitance allowable may vary from this value depending on the actual operating voltage and frequency of the application (I^2C Bus Specification Rev. 03, 19 June 2007).

Note 11: I^2C communication should not take place for the max t_{OSCWUP} time following a power-on reset.

Note 12: Data retention is tested in compliance with JESD47G.

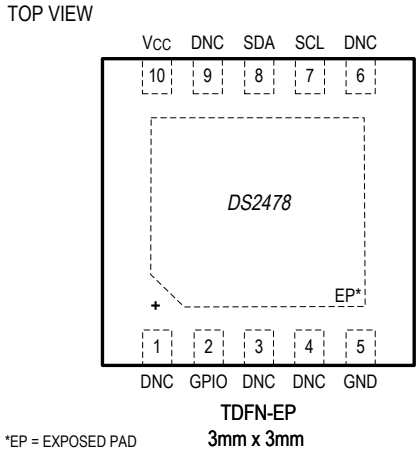
Typical Operating Characteristics

(V_{PUP} = +3.3V; T_A = T_{MIN} to T_{MAX} unless otherwise noted.)



Pin Configuration

10 TDFN



Pin Description

PIN	NAME	FUNCTION
1, 3, 4, 6, 9	DNC	Do Not Connect
2	GPIO	General-Purpose I/O
5	GND	Ground
7	SCL	I^2C Serial Clock Input. This pin must be connected to V_{CC} through a pullup resistor.
8	SDA	I^2C Serial Data Input/Output, Open-Drain. This pin must be connected to V_{CC} through a pullup resistor.
10	V_{CC}	Supply Voltage

Pin Description (continued)

PIN	NAME	FUNCTION
—	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.

Detailed Description

The DS2478 is a secure coprocessor that supports multiple asymmetric (ECC P-256) and symmetric (SHA-256) security functions for the DS28C40/DS28E40. In addition to the security services provided by the hardware-implemented ECC and SHA-256 engines, the device integrates a FIPS/NIST true random number generator (TRNG), 6Kb of secured OTP (3Kb user, 3Kb keys/secrets), one configurable GPIO pin, and a unique 64-bit serial number. The ECC public/private key capabilities operate from the NIST-defined P-256 curve and include FIPS 186-compliant ECDSA signature generation and verification for bidirectional asymmetric key authentication. Additionally, through FIPS/NIST 800-56B ECDH-based key agreement, the device supports secure storage and host communication of sensitive data, such as application-specific crypto keys that would be used independently by a host processor. The SHA-256 secret-key capabilities are compliant with FIPS 180 and are flexibly used either in conjunction with ECDSA operations or independently for multiple MAC and HMAC functions. Through the integrated TRNG, the device further enhances system crypto functionality with the ability to supply FIPS-grade random numbers to a host processor along with internal-only functions, including nonce values for ECDSA operation and optional generation of its ECC private keys. A GPIO pin can be operated under command control and include configurability supporting authenticated and nonauthenticated operation, including an ECDSA-based crypto-robust mode to support the secure-boot of a host processor.

The DS2478 integrates 6Kb of secured OTP memory to store keys, certificates, general-purpose data (four public/private key pairs, two secret keys) and control registers. Multiple user-programmable protection modes exist for the general-purpose memory space including ECDSA R/W authentication protection, SHA-256 HMAC R/W authentication protected, HMAC R/W encryption in conjunction with an ECDH established key, and unprotected. With these options, general-purpose memory can be flexibly configured to store end application data ranging from nonsensitive calibration constants to critically sensitive host-system crypto keys.

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 up to 100kbps in standard mode and up to 400kbps in fast mode. The DS2478 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 (see Figure 1). 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 DS2478 responds is shown in Figure 2. 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).

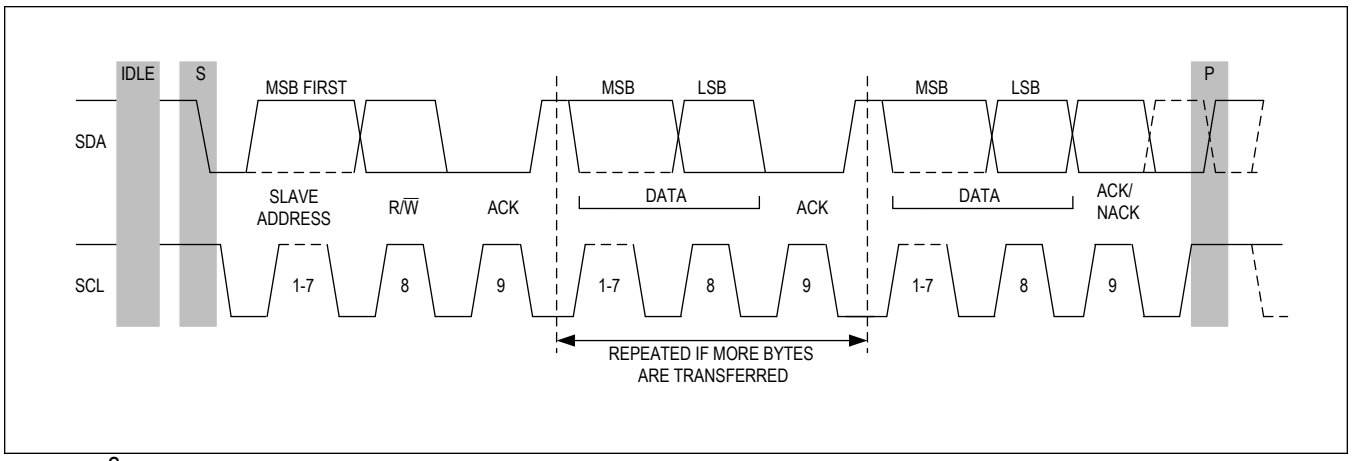


Figure 1. I²C Protocol Overview

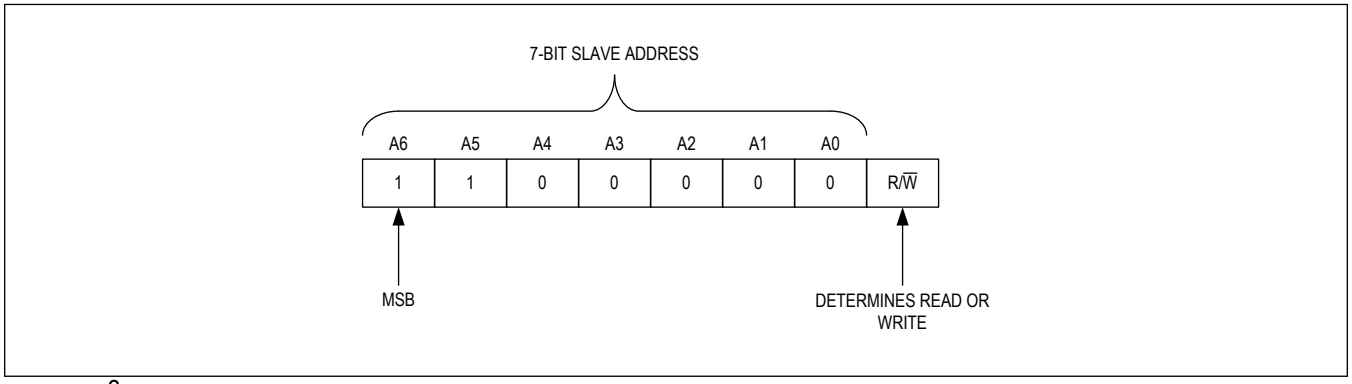


Figure 2. I²C Slave Address

I²C Definitions

The following terminology is commonly used to describe I²C data transfers. The timing references are defined in Figure 3.

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 3). 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 3) 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.

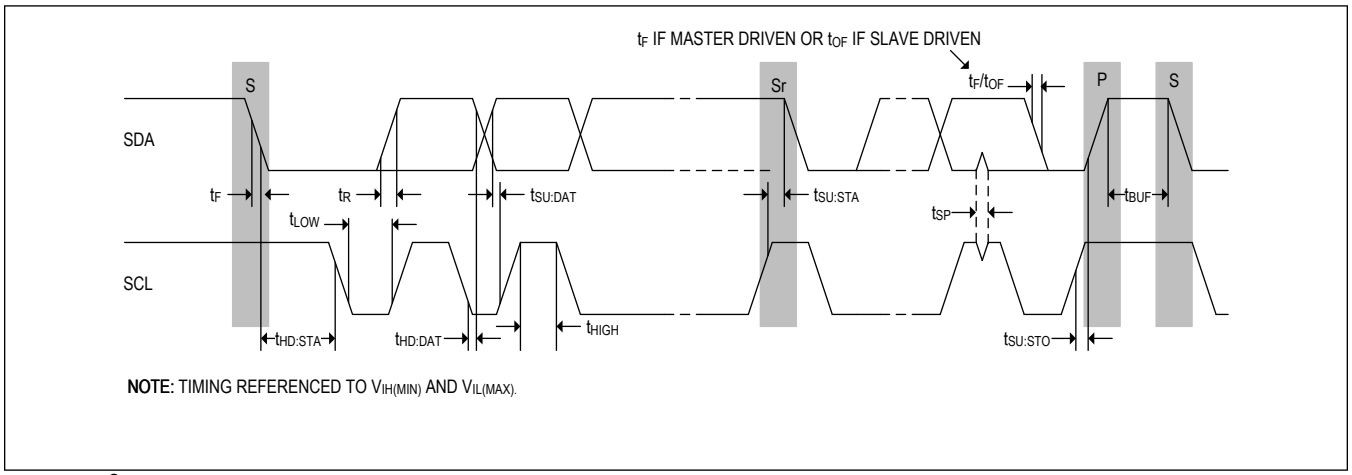
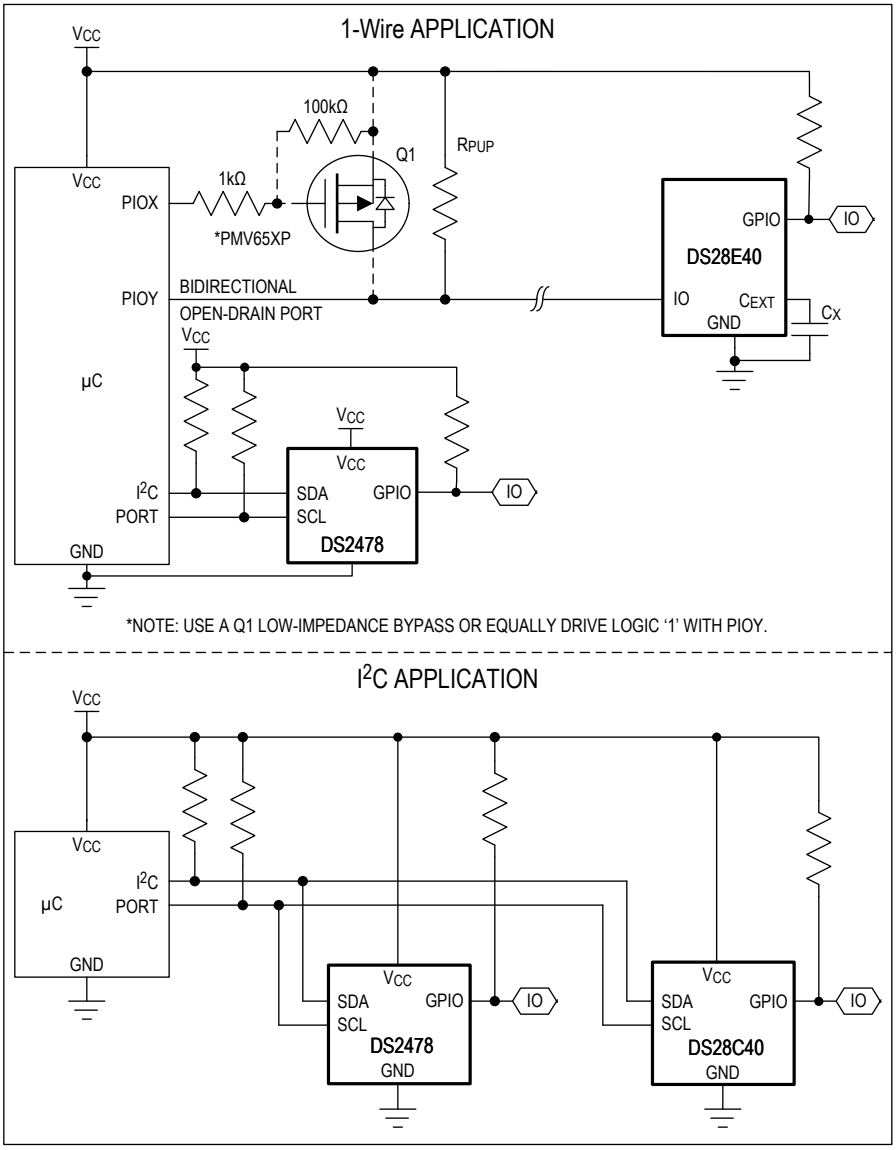


Figure 3. I^2C Timing Diagram

Typical Application Circuit



Ordering Information

PART NUMBER	TEMP RANGE	PIN-PACKAGE
DS2478ATB/VY+T	-40°C to +125°C	10 TDFN T1033Y+2 (2.5k pcs reel)

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

/V = Denotes an automotive-qualified part.

Y = Side-wettable TDFN package.

T = Tape and reel.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	1/22	Initial release	—

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Maxim Integrated:

DS2478ATB/VY+ DS2478ATB/VY+T