ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

DS2476 DeepCover Secure Coprocessor

General Description

The DS2476 is a secure ECDSA and HMAC SHA-256 coprocessor companion to the DS28C36. The coprocessor can compute any required HMACs or ECDSA signatures to do any operation on the DS28C36. The DS2476 provides a core set of cryptographic tools derived from integrated asymmetric (ECC-P256) 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 (RNG), 8Kb of secured EEPROM, a decrement-only counter, two pins of 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 either in conjunction with ECDSA operations or independently for multiple HMAC functions.

Two GPIO pins can be independently 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 active die shield, encrypted storage of keys, and algorithmic methods.

Applications

- IoT Node Crypto-Protection
- Accessory and Peripheral Secure Authentication
- Secure Storage of Cryptographic Keys for a Host Controller
- Secure Boot or Download of Firmware and/or System Parameters

Benefits and Features

- ECC-256 Compute Engine
  - FIPS 186 ECDSA P256 Signature and Verification
  - ECDH Key Exchange with Authentication Prevents Man-in-the-Middle Attacks
  - ECDSA Authenticated R/W of Configurable Memory
- FIPS 180 SHA-256 Compute Engine
  - HMAC
- SHA-256 OTP (One-Time Pad) Encrypted R/W of Configurable Memory Through ECDH Established Key
- Two GPIO Pins 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
- RNG with NIST SP 800-90B Compliant Entropy Source with Function to Read Out
- Optional Chip Generated Pr/Pu Key Pairs for ECC Operations
- 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
- 8Kbits of EEPROM 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, 100kHz and 400kHz
- Operating Range: 3.3V ±10%, -40°C to +85°C
- 6-Pin TDFN Package

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

***Typical Application Circuit* appears at end of data sheet.**

19-8589; Rev 0; 7/16

maxim integrated™

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND .....-0.5V to 4.0V
Maximum Current into Any Pin.....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.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}		2.97	3.3	3.63	V
Active Supply Current	I_{CC}	(Note 2)			300	µA
Standby Supply Current	I_{CCS}				250	µA
Computation Current	I_{CMP}	Refer to full data sheet				mA
GPIO						
Output Low	PIO V_{OL}				0.4	V
Input Low	PIO V_{IL}		-0.3		V_{CC} x 0.3V	V
Input High	PIO V_{IH}		V_{CC} x 0.7V		V_{CC} + 0.3V	V
Leakage current	I_L		-10		+10	µA
ECC ENGINE						
Generate ECDSA Signature Time	t_{GES}	Refer to full data sheet				ms
Generate ECC Key Pair	t_{GKP}					ms
Coprocessor ECDSA Verify Signature or Compute ECDH Time	t_{VES}					ms
SHA-256 ENGINE						
Computation Time (HMAC or RNG)	t_{CMP}	Refer to full data sheet				ms
EEPROM						
W/E Endurance	NCY	(Notes 4, 5)	100K			—
Read Memory Time	t_{RM}				1	ms
Write Memory Time	t_{WM}				15	ms
Data Retention	t_{DR}	T_A = +85°C (Notes 6, 7)	10			years
I²C SCL AND SDA PINS (Note 8)						
Low-Level Input Voltage	V_{IL}		-0.3		0.15 × V_{CC}	V
High-Level Input Voltage	V_{IH}		0.7 × V_{CC}		V_{CC} + 0.3V	V
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 9)		0.05 × V_{CC}		V
Low-Level Output Voltage at 4mA Sink Current	V_{OL}				0.4	V

Electrical Characteristics (continued)

(T_A = -40°C to +85°C.) (Note 1)

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 9)		30		ns
Pulse Width of Spikes that are Suppressed by the Input Filter	t_{SP}	(Note 9)			50	ns
Input Current with an Input Voltage Between 0.1VCCmax and 0.9VCCmax	II		-10		+10	µA
Input Capacitance	CI	(Note 9)		10		pF
SCL Clock Frequency	f_{SCL}	(Note 10)	0		400	kHz
Hold Time (Repeated) START Condition	$t_{HD:STA}$	After this period, the first clock pulse is generated	0.6			µs
LOW Period of the SCL Clock	t_{LOW}		1.3			µs
HIGH Period of the SCL Clock	t_{HIGH}		0.6			µs
Setup Time for a Repeated START Condition	$t_{SU:STA}$		0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 9, 11, 12)			0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Note 13)	100			ns
Setup Time for STOP Condition	$t_{SU:STO}$		0.6			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}		1.3			µs
Capacitive Load for Each Bus Line	C_B	(Notes 10, 14)			400	pF
Warm-Up Time	t_{OSCWUP}	(Note 15)			250	µs

Note 1: 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 at +25°C

Note 2: Operating current continuously reading memory at 400kHz with < 25ns rise and fall times on SDA and SCL.

Note 3: Refer to full data sheet.

Note 4: Write-cycle endurance is tested in compliance with JESD47H.

Note 5: Not 100% production tested; guaranteed by reliability qualification.

Note 6: Data retention is tested in compliance with JESD47H.

Note 7: 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 8: All I^2C timing values are referred to $V_{IH(MIN)}$ and $V_{IL(MAX)}$ levels, except for t_{OF}, whichis measured from $V_{IH(MIN)}$ to 0.3 x V_{CC}.

Note 9: Guaranteed by design and/or characterization only. Not production tested.

Note 10: System requirement.

Note 11: The DS2476 provides a hold time of at least 100ns for the SDA signal (referred to the $V_{IH(MIN)}$ of the SCL signal) to bridge the undefined region of the falling edge of SCL. The master can provide a hold time of 0ns when writing to the device.

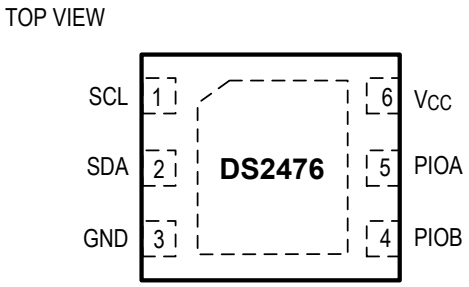
Note 12: The maximum $t_{HD:DAT}$ has only to be met if the device does not stretch the LOW period (t_{LOW}) of the SCL signal. If the clock stretches the SCL, the data must be valid by the set-up time before it releases the clock (I^2C-bus specification Rev. 03, 19 June 2007).

Note 13: A fast-mode I^2C-bus device can be used in a standard-mode I^2C-bus system, but the requirement $t_{SU:DAT} \geq$ 250ns must then be met. This is automatically the case if the device does not stretch the low period of the SCL signal. If such a device does stretch the low period of the SCL signal, it must output the next data bit to the SDA line tr max + $t_{SU:DAT}$ = 1000 + 250 = 1250ns (according to the standard-mode I^2C-bus specification) before the SCL line is released. Also, the acknowledge timing must meet this set-up time. (I^2C-bus specification Rev. 03, 19 June 2007)

Note 14: C_B = total capacitance of one bus line in pF. The maximum bus capacitance allowable can 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 15: I^2C communication should not take place for max t_{OSCWUP} time following a power-on reset.

Pin Configuration



TDFN-EP
(3mm x 3mm)

Pin Description

PIN	NAME	FUNCTION
1	SCL	I^2C CLK
2	SDA	I^2C Data
3	GND	Ground
4	PIOB	General-Purpose IO
5	PIOA	General-Purpose IO
6	V_{CC}	Supply Voltage
—	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.

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 of up to 100kbps in standard mode and up to 400kbps in fast mode. The DS2476 works in both modes.

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 41). 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 DS2476 responds is shown in Figure 42. 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).

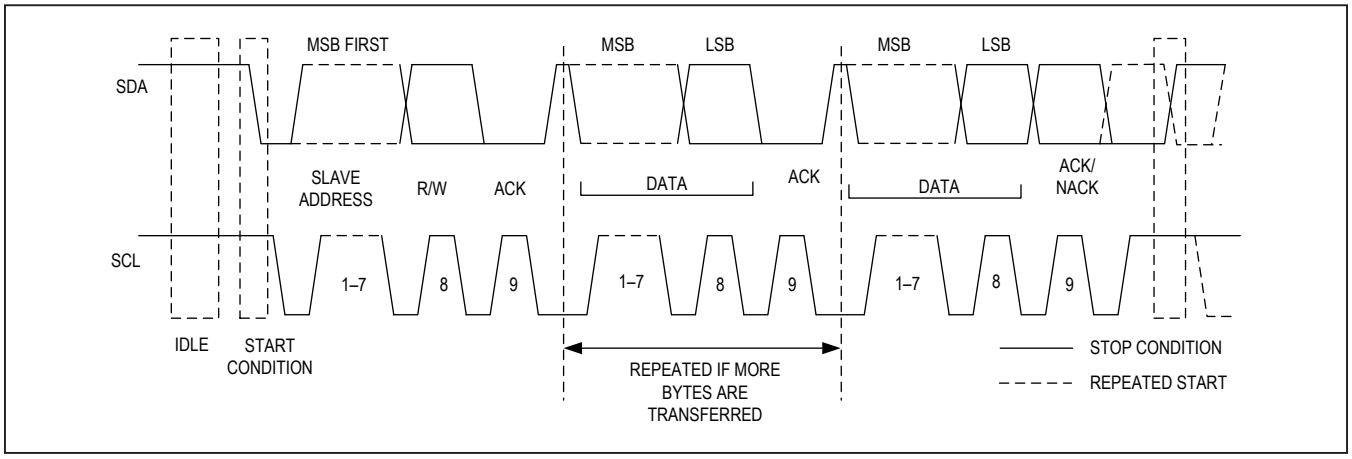


Figure 41. I²C Protocol Overview

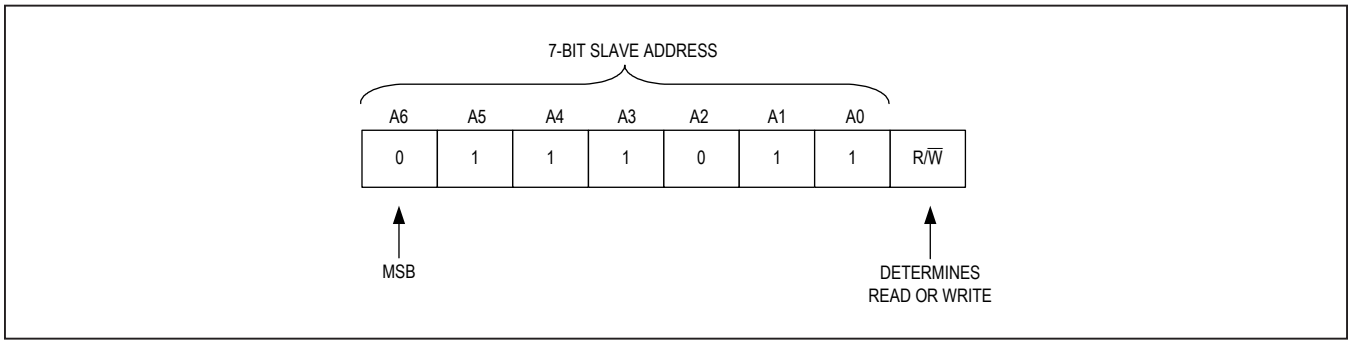


Figure 42. DS2476 I²C Slave Address

I²C Definitions

The following terminology is commonly used to describe I²C data transfers. The timing references are defined in Figure 43.

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 43). 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 43) 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.

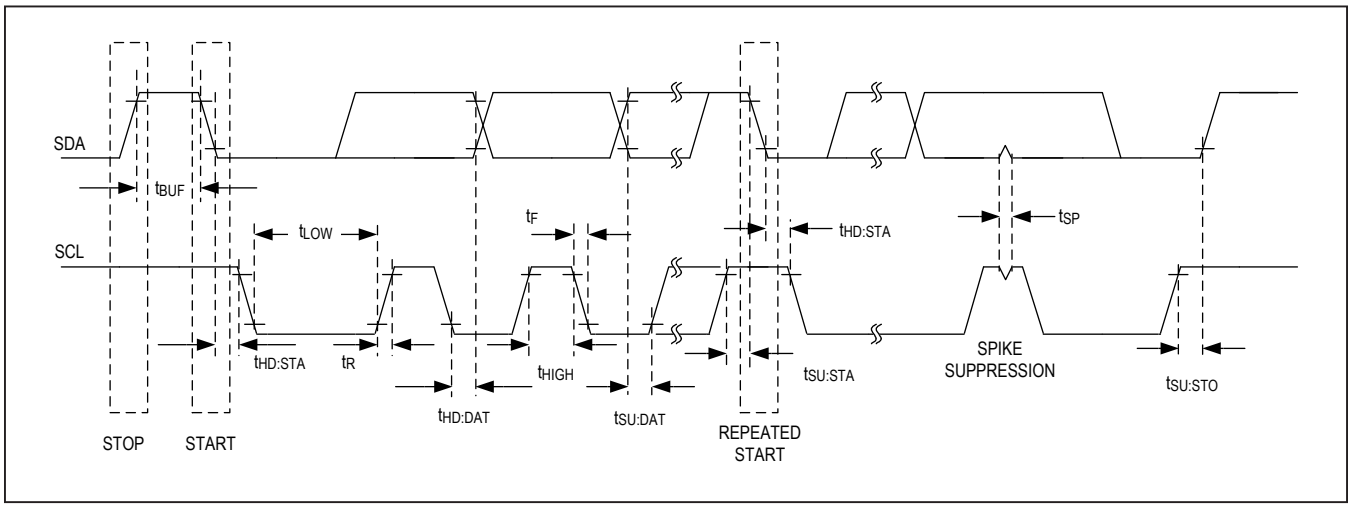


Figure 43: I²C Timing Diagram

Acknowledged by Slave

A slave device, when addressed, is usually obliged to generate an acknowledge after the receipt of each byte. The master must generate the clock pulse for each acknowledge bit. A slave that acknowledges must pull down the SDA line during the acknowledge clock pulse so that it remains stable low during the high period of this clock pulse. Setup and hold times $t_{SU:DAT}$ and $t_{HD:DAT}$ must be taken into account.

Acknowledged by Master

To continue reading from a slave, the master is obliged to generate an acknowledge after the receipt of each byte. The master must generate the clock pulse for each acknowledge bit. A master that acknowledges must pull down the SDA line during the acknowledge clock pulse so that it remains stable low during the high period of this clock pulse. Setup and hold times $t_{SU:DAT}$ before the rising edge of SCL and $t_{HD:DAT}$ after the falling edge of SCL must be taken into account.

Not Acknowledged by Slave

A slave device may be unable to receive or transmit data, for example, because it is busy performing a real-time function such as MAC computation or EEPROM write cycle or is in sleep mode. In this case, the slave does not acknowledge its slave address and leaves the SDA line high. A slave that is ready to communicate acknowledges at least its slave address. However, some time later, the slave might refuse to accept data, possibly because of an invalid command code or unexpected data. In this case, the slave device does not acknowledge any of the bytes that it refuses and leaves SDA high. In either case, after a slave has failed to acknowledge, the master first should generate a repeated START condition or a STOP condition followed by a START condition to begin a new data transfer.

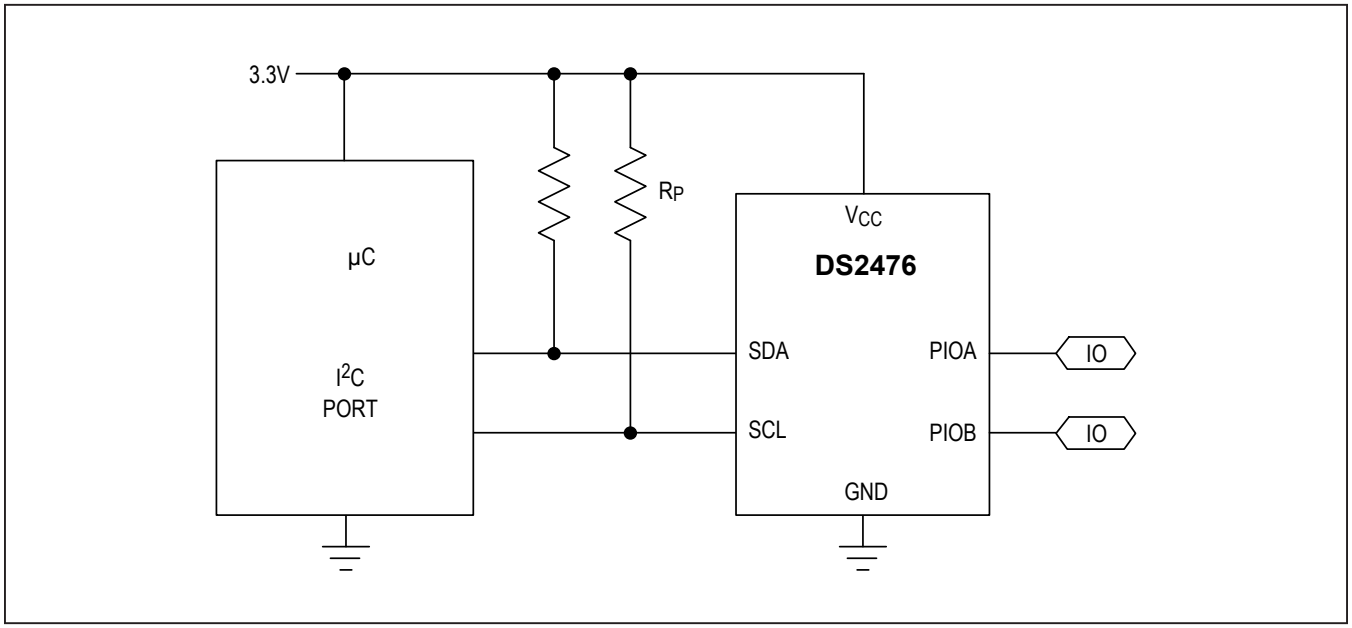
Not Acknowledged by Master

At some time when receiving data, the master must signal an end of data to the slave. To achieve this, the master does not acknowledge the last byte that it has received from the slave. In response, the slave releases SDA, allowing the master to generate the STOP condition.

Read and Write

To write to the DS2476, the master must access the device in write access mode, i.e., the slave address must be sent with the direction bit set to 0. The next byte to be sent in write access mode is command byte. To read from the DS2476, the master must access the device in read access mode, i.e., the slave address must be sent with the direction bit set to 1. The read address is determined either from a preceding write access or implied from a function command.

Typical Application Circuit



Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS2476Q+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

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.

