ABRIDGED DATA SHEET

DS2475

DeepCover ECDSA Host Processor with 1-Wire Master

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 Elliptic Curve Digital Signature Algorithm (ECDSA) coprocessor with built-in 1-Wire® master (DS2475) enables the efficient implementation of public-key based authentication when combined with an ECDSA secure authenticator. Additionally, for operation with 1-Wire ECDSA authenticators, an I²C-to-1-Wire protocol conversion function relieves the system host processor from generating time-critical 1-Wire waveforms. The DS2475 interfaces directly to standard (100kHz max) or fast (400kHz max) I²C masters. When not in use, the DS2475 can be put in sleep mode where power consumption is minimal.

Applications

- Authentication of Accessories
- Peripheral Authentication
- Authentication of Consumables

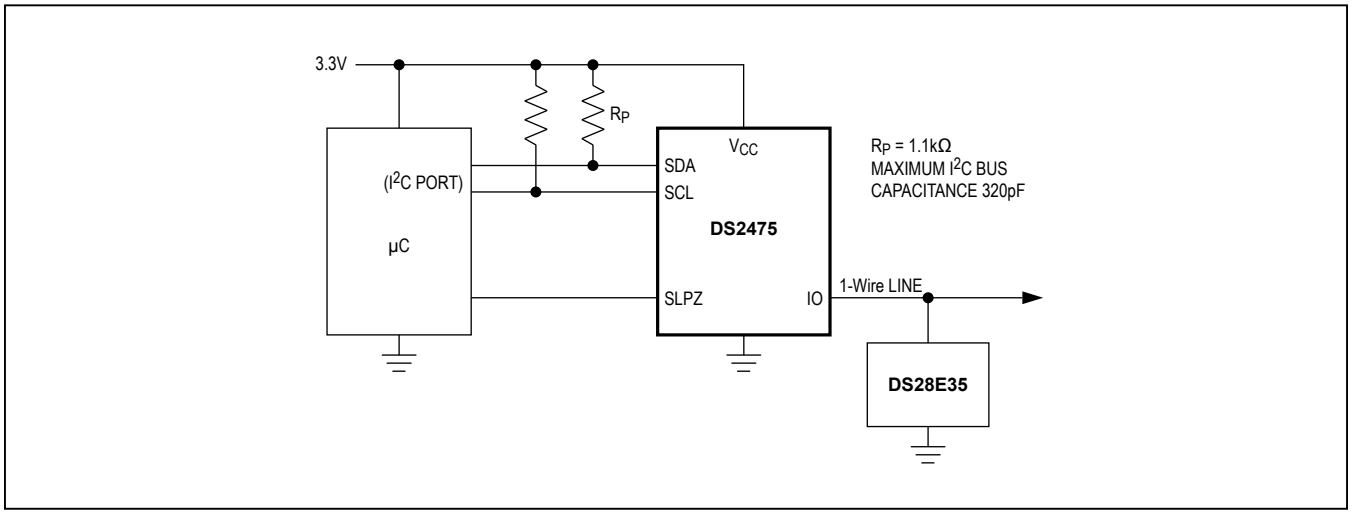
Benefits and Features

- High-Speed ECDSA Engine for Public-Key Signature Verification
- Implements NIST FIPS 186-Based ECDSA Algorithm
- Integrated NIST FIPS 180 SHA-256 Engine for Efficient ECDSA Input Data Computation
- 1-Wire Line Driver Supporting Both Standard and Overdrive Communication Speeds
- Supports Power-Saving Sleep Mode (SLPZ Pin)
- ±8kV ESD Protection on IO to GND (JESD22-A114 HBM, typ)
- Operating Range: 3.3V ±10%, -40°C to +85°C
- 6-Pin SOT23 Package

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

For related parts and recommended products to use with this part, refer to www.maximintegrated.com/DS2475.related.

Typical Application Circuit



DeepCover and 1-Wire are registered trademarks of Maxim Integrated Products, Inc.

219-0043; Rev 0; 6/14

maxim integrated™

DS2475

DeepCover ECDSA Host Processor with 1-Wire Master

Absolute Maximum Ratings

IO 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.

Package Thermal Characteristics (Note 1)

SOT23
Junction-to-Ambient Thermal Resistance (θ_{JA}) .....74.60°C/W
Junction-to-Case Thermal Resistance (θ_{JC}).....6°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 = -40°C to +85°C, unless otherwise noted) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}		2.97	3.3	3.63	V
Supply Current (Note 3)	I_{CC}	(Note 4)		1.2	2	mA
		Sleep mode (SLPZ = 0.0V), V_{CC} = 3.63V		50	150	nA
1-Wire Input High	V_{IH1}		0.6 × V_{CC}			V
1-Wire Input Low	V_{IL1}				0.2 × V_{CC}	V
1-Wire Weak Pullup Resistor (Notes 5, 6)	R_{WPU}	Low range	375	500	750	Ω
		High range	750	1000	1350	
1-Wire Output Low (Note 3)	V_{OL1}	V_{CC} = 2.97V, 8mA sink current			0.25	V
Active Pullup On Threshold	V_{IAPO}	(Note 5)		0.95	1.2	V
Active Pullup On Time (Notes 5, 7)	t_{APU}	1-Wire time slot	See APU bit description			µs
		1-Wire reset standard speed	2.13	2.5	2.88	
		1-Wire reset overdrive speed	0.43	0.5	0.58	
Active Pullup Impedance	R_{APU}	V_{CC} = 2.97V, 4mA load (Note 5)			60	Ω
1-Wire Output Fall Time (Note 5)	t_F	Standard	0.25		1	µs
		Overdrive	0.05		0.2	
IO PIN: 1-Wire TIMING (Note 8)						
Reset Low Time	t_{RSTL}	Standard and overdrive	-15%	See Table 6	+15%	µs
Reset High Time	t_{RSTH}	Standard and overdrive	Equal to t_{RSTL}			µs
Presence-Detect Sample Time	t_{MSP}	Standard and overdrive	-15%	See Table 6	+15%	µs

Electrical Characteristics (continued)

(T_A = -40°C to +85°C, unless otherwise noted) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Sampling for Short and Interrupt	t_{SI}	Standard	6.8	8	9.2	µs
		Overdrive	1.2	2	2.3	
Write-1/Read Low Time	t_{W1L}	Standard	6.4	8	9.6	µs
		Overdrive	-15%	See Table 6	+15%	
Read Sample Time	t_{MSR}	Standard	10.2	12	13.8	µs
		Overdrive	1.28	1.5	1.73	
Write-0 Low Time	t_{W0L}	Standard and overdrive	-15%	See Table 6	+15%	µs
Write-0 Recovery Time	t_{REC0}	Standard and overdrive	-15%	See Table 6	+15%	µs
1-Wire Time Slot	t_{SLOT}	Standard and overdrive	Equal to t_{W0L} + t_{REC0}			µs
ECDSA ENGINE						
Computation Current	I_{ECE}	Refer to the full datasheet				mA
Public Key Computation Time	t_{CPK}					ms
Signature Verification Time	t_{VS}					ms
SLPZ PIN						
Low Level Input Voltage	V_{IL}	(Note 5)	-0.5		0.3 × V_{CC}	V
High Level Input Voltage	V_{IH}		0.7 × V_{CC}		V_{CC} + 0.5V	V
Input Leakage Current	I_I	Pin at 3.63V (Note 5)			0.1	µA
Wake-Up Time from Sleep Mode	t_{SWUP}	(Note 10)			150	µs
I^2C PINS (Note 11)						
Low Level Input Voltage	V_{IL}		-0.5		0.3 × V_{CC}	V
High Level Input Voltage	V_{IH}		0.7 × V_{CC}			V
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 5)	0.05 × V_{CC}			V
Low Level Output Voltage at 3mA Sink Current (SDA Only)	V_{OL}	(Note 3)			0.4	V
Output Fall Time from V_{IHMIN} to V_{ILMAX} with a Bus Capacitance from 10pF to 400pF	t_{OF}	(Note 5)	60		250	ns
Pulse Width of Spikes that are Suppressed by the Input Filter	t_{SP}	(Note 5)			30	ns
Input Current with an Input Voltage Between 0.1V_{CCMAX} and 0.9V_{CCMAX}	I_I	(Notes 5, 12)	-10		10	µA

Electrical Characteristics (continued)

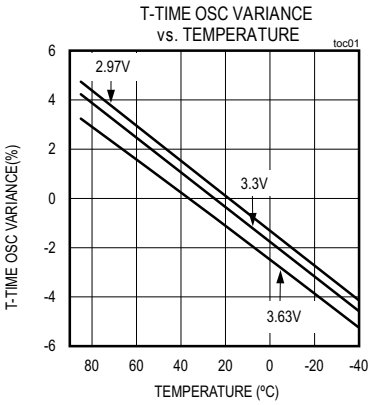
(T_A = -40°C to +85°C, unless otherwise noted) (Note 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Input Capacitance	C_I	(Note 5)			10	pF
SCL Clock Frequency	f_{SCL}		0		400	kHz
Hold Time (Repeated) START Condition; After this Period, the First Clock Pulse is Generated	$t_{HD:STA}$	(Note 5)	0.6			µs
Low Period of the SCL Clock	t_{LOW}	(Note 5)	1.3			µs
High Period of the SCL Clock	t_{HIGH}	(Note 5)	0.6			µs
Setup Time for a Repeated START Condition	$t_{SU:STA}$	(Note 5)	0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 5, 13, 14)			0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Notes 5, 15)	250			ns
Setup Time for STOP Condition	$t_{SU:STO}$	(Note 5)	0.6			µs
Bus Free Time Between a STOP and START Condition	t_{BUF}	(Note 5)	1.3			µs
Capacitive Load for Each Bus Line	C_B	(Notes 5, 16)			400	pF

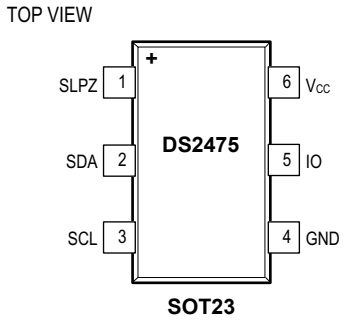
Note 2: Limits are 100% production tested at T_A = +25°C and T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values are at 25°C.
Note 3: Production tested at T_A = +85°C only.
Note 4: Operating current with 1-Wire write byte sequence followed by continuous read of 1-Wire Master Status register at 400kHz in overdrive.
Note 5: Guaranteed by design and/or characterization only; not production tested.
Note 6: Active pullup or resistive pullup and range are configurable.
Note 7: The active pullup does not apply to the rising edge of a presence pulse outside of a 1-Wire Reset Pulse command or during the recovery after a short on the 1-Wire line.
Note 8: All 1-Wire timing specifications are derived from the same timing circuit (i.e., T-TIME OSC).
Note 9: Refer to the full datasheet.
Note 10: I^2C communication should not take place for the max t_{OSCWUP} or t_{SWUP} time following a power-on reset or a wake-up from sleep mode.
Note 11: All I^2C timing values are referred to V_{IHMIN} and V_{ILMAX} levels.
Note 12: I/O pins of the DS2475 do not obstruct the SDA and SCL lines if V_{CC} is switched off.
Note 13: The DS2475 provides a hold time of at least 300ns for the SDA signal (referred to the V_{IHMIN} of the SCL signal) to bridge the undefined region of the falling edge of SCL.
Note 14: 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 setup time before it releases the clock (I^2C bus specification Rev. 03, 19 June 2007).
Note 15: 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 $t_{RMAX} + t_{SU:DAT} = 1000 + 250 = 1250ns$ (according to the standard-mode I^2C bus specification) before the SCL line is released. Also, the acknowledge timing must meet this setup time (I^2C bus specification Rev. 03, 19 June 2007).
Note 16: 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).

Typical Operating Characteristics

(V_{GND} = 0V.)



Pin Configuration



Pin Description

PIN	NAME	FUNCTION
1	SLPZ	Active-Low Control Input for Sleep Mode. Activates the low-power sleep mode and issues a device reset.
2	SDA	I^2C Serial Data Input/Output. Must be connected to V_{CC} through a pullup resistor.
3	SCL	I^2C Serial Clock Input. Must be connected to V_{CC} through a pullup resistor.
4	GND	Ground Reference
5	IO	I/O Driver for 1-Wire Line
6	V_{CC}	Power-Supply Input

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS2475R+U	-40°C to +85°C	6 SOT23
DS2475R+T	-40°C to +85°C	6 SOT23 (3k pcs)

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

T = Tape and reel.

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 SOT23	U6SN+1	21-0058	90-0175