ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

DS28C22

DeepCover Secure Memory with I²C SHA-256 and 3Kb User EEPROM

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 Secure Memory (DS28C22) combines crypto-strong, bidirectional, secure challenge-and-response authentication and small message encryption functionality with an implementation based on the FIPS 180-specified Secure Hash Algorithm (SHA-256). A 3Kb user-programmable EEPROM array provides nonvolatile storage for application data and additional protected memory holds a read-protected secret for SHA-256 operations and settings for user memory control. Each device has its own guaranteed unique and unalterable 64-bit ROM identification number (ROM ID) that is factory programmed into the chip. This unique ROM ID is used as a fundamental input parameter for cryptographic operations and also serves as an electronic serial number within the application. A bidirectional security model enables two-way authentication and encryption between a host system and slave-embedded DS28C22. Slave-to-host authentication is used by a host system to securely validate that an attached or embedded DS28C22 is authentic. Host-to-slave authentication is used to protect DS28C22 user memory from being modified by a nonauthentic host. The SHA-256 message authentication code (MAC), which the DS28C22 generates, is computed from data in the user memory, an on-chip secret, a host random challenge, and the 64-bit ROM ID. The device also facilitates encrypted read and write between host and slave using a one time pad computed by the SHA-256 engine. When not in use, the DS28C22 can be put in sleep mode where power consumption is minimal.

Applications

- Authentication of Network-Attached Appliances
- System Intellectual Property Protection
- Secure Feature Setting for Configurable Systems
- Key Generation and Secure Exchange for Cryptographic Systems

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

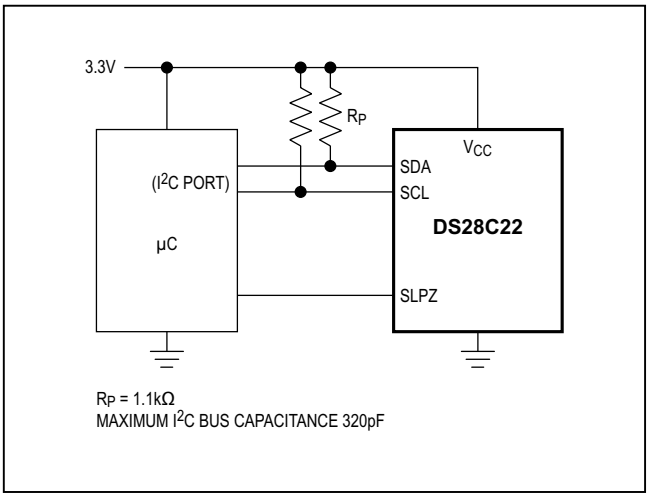
Benefits and Features

- Symmetric Key-Based Bidirectional Secure Authentication and Encryption Model Based on SHA-256
- Dedicated Hardware-Accelerated SHA Engine for Generating SHA-256 MACs
- Strong Authentication with a 256-Bit, User-Programmable Secret, and Input Challenge
- 3072 Bits of User EEPROM Partitioned Into 12 Pages of 256 Bits
- User-Programmable and Irreversible EEPROM Protection Modes Including Authentication, Write and Read Protect, Encryption, and OTP/EPROM Emulation
- Supports 100kHz and 400kHz I²C Communication Speeds
- Supports Power-Saving Sleep Mode at 0.5µA (typ)
- Operating Range: 3.3V ±10%, -40°C to +85°C
- 8-Pin TDFN 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/DS28C22.related.

Typical Application Circuit



219-0029; Rev 2; 7/13

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.

Package Thermal Characteristics (Note 1)

TDFN
Junction-to-Ambient Thermal Resistance (θ_{JA}) .....60°C/W
Junction-to-Case Thermal Resistance (θ_{JC}).....11°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	I_{CC}	(Note 3)			750	µA
		Sleep mode (SLPZ pin low), V_{CC} = 3.63V		0.5	2.0	
SHA-256 Engine						
Computation Current	I_{CSHA}	**Refer to the full data sheet.**				mA
Computation Time	t_{CSHA}					ms
EEPROM						
Programming Current	I_{PROG}	(Notes 4, 5)			2	mA
Programming Time for 32-Bit Segment	t_{PROG}	**Refer to the full data sheet.**				ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 6, 7)	1000			—
Data Retention	t_{DR}	T_A = +85°C (Notes 8, 9, 10)	10			years
SLPZ Pin						
LOW Level Input Voltage	V_{IL}		-0.5		0.3 x V_{CC}	V
HIGH Level Input Voltage	V_{IH}		0.7 x V_{CC}		V_{CC} + 0.5V	V
Input Leakage Current	I_I	Pin at 3.63V			0.1	µA
Wakeup Time from Sleep Mode	t_{SWUP}	(Note 11)			250	µs
I²C SCL and SDA Pins (Note 12)						
LOW Level Input Voltage	V_{IL}		-0.5		0.3 x V_{CC}	V
HIGH Level Input Voltage	V_{IH}		0.7 x V_{CC}		$V_{CC(MAX)}$ + 0.5V	V

Electrical Characteristics (continued)

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

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 4)	0.05 x V_{CC}			V
LOW Level Output Voltage at 3mA Sink Current	V_{OL}				0.4	V
Output Fall Time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$ with Bus Capacitance from 10pF to 400pF	t_{OF}	(Note 4)	60		300	ns
Pulse Width of Spikes Suppressed by the Input Filter	t_{SP}	(Note 4)			50	ns
Input Current with Input Voltage Between $0.1V_{CC(MAX)}$ and $0.9V_{CC(MAX)}$	I_I	(Notes 4, 13)	-10		+10	µA
Input Capacitance	C_I	(Note 4)			10	pF
SCL Clock Frequency	f_{SCL}		0		400	kHz
Hold Time (Repeated) START Condition, After This Period, First Clock Pulse Generated	$t_{HD:STA}$	(Note 4)	0.6			µs
LOW Period of the SCL Clock	t_{LOW}	(Note 4)	1.3			µs
HIGH Period of the SCL Clock	t_{HIGH}	(Note 4)	0.6			µs
Setup Time for Repeated START Condition	$t_{SU:STA}$	(Note 4)	0.6			µs
Data Hold Time	$t_{HD:DAT}$	(Notes 4, 14, 15)			0.9	µs
Data Setup Time	$t_{SU:DAT}$	(Notes 4, 16)	250			ns
Setup Time for STOP Condition	$t_{SU:STO}$	(Note 4)	0.6			µs
Bus Free Time Between STOP and START Condition	t_{BUF}	(Note 4)	1.3			µs
Capacitive Load for Each Bus Line	C_b	(Notes 4, 17)			400	pF
Oscillator Warm-Up Time	t_{OSCWUP}	(Note 11)			250	µs

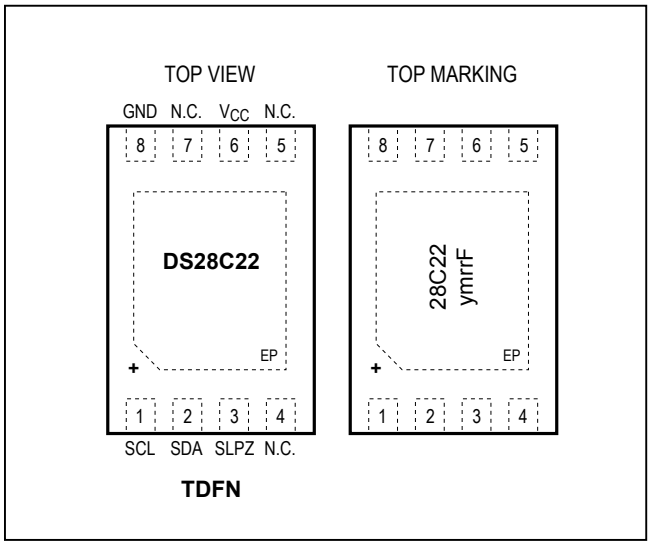
Note 2: Limits are 100% production tested at T_A = +25°C and T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization.
Note 3: Operating current continuously reading the Memory/MAC Read/Write Register at 400kHz.
Note 4: Guaranteed by design and/or characterization only. Not production tested.
Note 5: **Refer to the full data sheet.**
Note 6: Write-cycle endurance is tested in compliance with JESD47G.
Note 7: Not 100% production tested; guaranteed by reliability monitor sampling.
Note 8: Data retention is tested in compliance with JESD47G.
Note 9: 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 10: EEPROM Writes can become nonfunctional after the data-retention time is exceeded. Long-term storage at elevated temperatures is not recommended.
Note 11: I²C 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.

Electrical Characteristics (continued)

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

Note 12: All I²C timing values are referred to $V_{IH(MIN)}$ and $V_{IL(MAX)}$ levels.
Note 13: I/O pins of the DS28C22 do not obstruct the SDA and SCL lines if V_{CC} is switched off.
Note 14: The DS28C22 provides a hold time of at least 300ns 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.
Note 15: 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. (I²C-bus specification Rev. 03, 19 June 2007)
Note 16: A fast-mode I²C-bus device can be used in a standard-mode I²C-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 I²C-bus specification) before the SCL line is released. Also the acknowledge timing must meet this setup time. (I²C-bus specification Rev. 03, 19 June 2007)
Note 17: 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)

Pin Configuration



TDFN

Pin Description

PIN	NAME	FUNCTION
1	SCL	I²C Serial Clock Input. Must be connected to V_{CC} through a pullup resistor.
2	SDA	I²C Serial Data Input/Output. Must be connected to V_{CC} through a pullup resistor.
3	SLPZ	Active-low control input to activate the low-power sleep mode, and to issue a device reset.
4, 5, 7	N.C.	No Connection
6	V_{CC}	Power-Supply Input
8	GND	Ground Reference
—	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.