DS28S60

DeepCover Cryptographic Coprocessor with ChipDNA

General Description

The DS28S60 DeepCover® cryptographic coprocessor easily integrates into embedded systems enabling confidentiality, authentication and integrity of information. With a fixed command set and no device-level firmware development required, the DS28S60 makes it fast and easy to implement full security for IoT devices. Communication with the device is performed using the industry-standard SPI slave interface at up to 20Mbps with a simple set of commands that provide a comprehensive security toolbox utilizing hardware-based cryptographic blocks. As a coprocessor to an SPI-interfaced host controller, the command functionality includes ECDSA-P256 signature and verification, SHA-256 based digital signature, AES-128 packet encryption/decryption, ECDHE key exchange for session key generation, and access to high-quality random numbers. An NIST SP800-90B compliant true random number generator (TRNG) is integrated for on-chip cryptographic operations as well as providing random data and nonces to the host controller, if required. Nonvolatile storage for secrets, certificates, public/private keys, and application-specific sensitive data is supported with 3.6KB of secured flash memory.

The DS28S60 integrates Maxim's patented ChipDNA™ feature, a physically unclonable function (PUF) to provide a cost-effective solution with the ultimate protection against security attacks. Using the random variation of semiconductor device characteristics that naturally occur during wafer fabrication, the ChipDNA circuit generates a unique output value that is repeatable over time, temperature, and operating voltage. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, preventing discovery of the unique value used by the chip's cryptographic functions. ChipDNA output is utilized as key content to cryptographically secure all device-stored data.

Applications

- Internet of Things (IoT) Device Security
- Key Management and Exchange
- End-to-End Encryption
- End-Point Authentication
- Prevention of Counterfeit Products

Benefits and Features

- Secure Coprocessor with NIST-Compliant Hardware-Based Crypto
  - FIPS-180 SHA-256 MAC and FIPS-198 HMAC Hash
  - FIPS-197 AES-128 with GCM
  - FIPS-186 ECDSA-P256 Elliptic Curve Digital Signature/Verification
  - SP800-56A ECDHE-P256 Key Exchange
  - SP800-90B Compliant TRNG
- Robust Countermeasures Protect Against Security Attacks
  - ChipDNA Produced Key Cryptographically Protects All Stored Data
  - Actively Monitored Die Shield Detects and Reacts to Intrusion Attempts
- Enables Fast Time-to-Market with Easy End Application Integration
  - Fixed-Function Command Set, No Device-Level Firmware
  - C-Source Demos for Examples of SW Development
  - 3.6KB Flash Array for Secure Key, Certificate, and Data Storage
- High-Speed Interface for Host Microcontroller Communication
  - 20MHz SPI with Mode 0 or Mode 3 Operation
- Supplemental Features Enable Easy Integration into End Applications
  - Unique and Unalterable Factory-Programmed, 64-Bit Identification Number (ROM ID)
  - Low-Power Operation
    - 100nA Power-Down Mode
    - 0.35mA Idle
  - 12-Pin, 3mm x 3mm TDFN
- -40°C to +105°C, 1.62V to 3.63V

Request DS28S60 Security User Guide

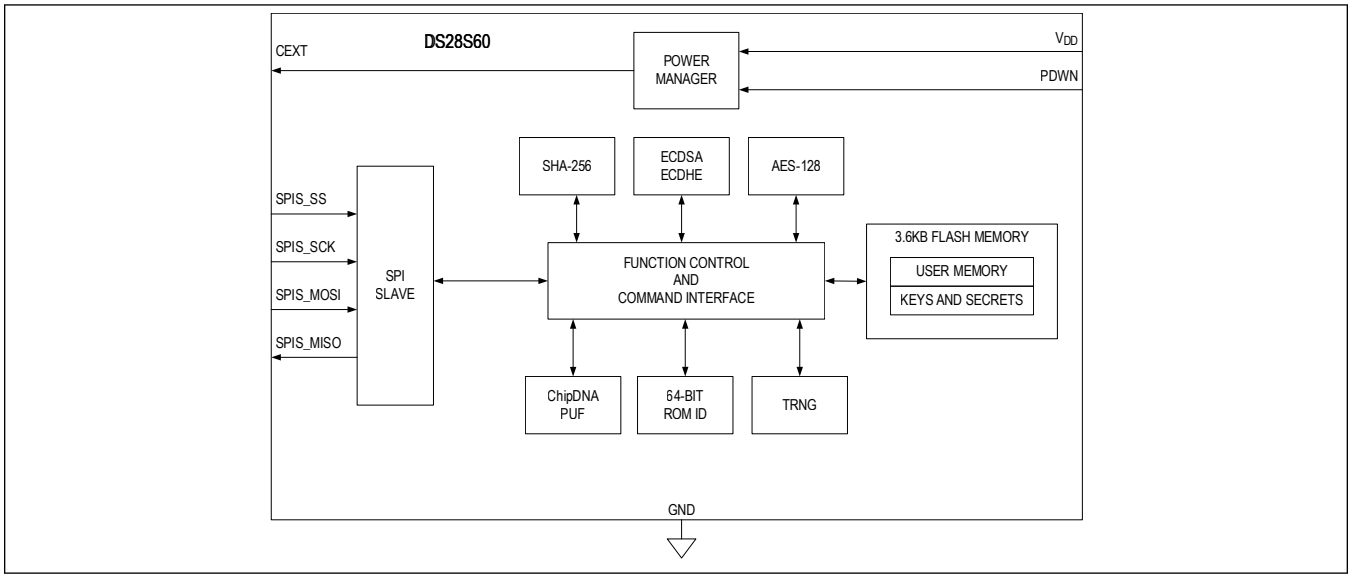
***Ordering Information* appears at end of data sheet.**

19-000793; Rev 1; 7/20

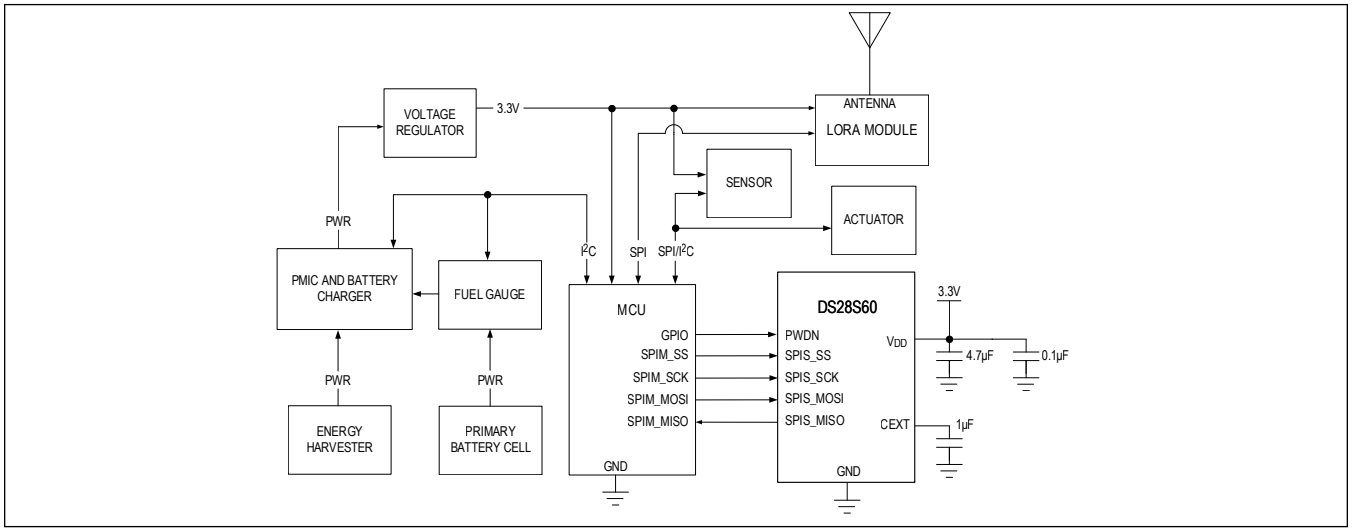
maxim integrated™

Functional Diagrams

DS28S60 Block Diagram



Typical Application Example, Battery-Powered LoRa Endpoint



Absolute Maximum Ratings

(All voltages with respect to GND, unless otherwise noted.).....
V_{DD} to GND..... -0.3V to 3.63V
Any Pin to GND except V_{DD}.....-0.3V to (V_{DD} + 0.3)V
Operating Temperature Range .....-40°C to +105°C
Storage Temperature Range.....-40°C to +150°C
Junction Temperature ..... +150°C
Soldering Temperature (reflow)..... +260°C

Continuous Package Power Dissipation 12-Pin TDFN (Single-Layer Board) T_A = +70°C, (derate 15.90mW/°C above +70°C).....1269.8 mW
Continuous Package Power Dissipation 12-Pin TDFN (Multilayer Board) T_A = +70°C (derate 24.40mW/°C above +70°C).....1951.2mW

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

12 TDFN

Package Code	TD1233+1C
Outline Number	21-0664
Land Pattern Number	90-0397
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	63°C/W
Junction to Case (θ_{JC})	8.5°C/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	41°C/W
Junction to Case (θ_{JC})	8.5°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 = +105ºC. 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
POWER SUPPLY						
Supply Voltage	V_{DD}	(*Note 1*)	1.62	3.3	3.63	V
Power-On Reset	V_{POR}			1.33		V
Active Current	I_A	T_A = +25°C, no I/O or cryptographic operation are active		1.28	3	mA
	I_{ECDSA}	T_A = +25°C, performing signature operation		1.62		
	I_{SHA}	T_A = +25°C, performing SHA-256 operation		0.95		
Idle Current	I_{IDLE}	T_A = +25°C, PDWN = V_{DD}, CPU/ peripherals inactive, I/O pins in inactive state		0.4		mA
Power-Down Current	I_{PDWN}	T_A = +25°C, V_{PDWN} = 0V, V_{DD} = 1.8V		100		nA

Electrical Characteristics (continued)

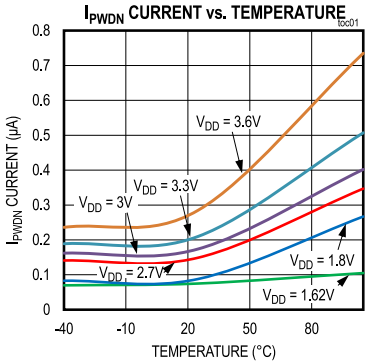
(Limits are 100% tested at T_A = +25ºC and T_A = +105ºC. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Specifications marked GBD are guaranteed by design and not production tested. Specifications to the minimum operating temperature are guaranteed by design and are not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Power-Down Resistance	R_{PDWN}	Pulldown to ground		1		MΩ
FUNCTIONAL TIMING						
Operation Time	t_{OP}				1	ms
Wake-Up Time	t_{WAKEUP}				2	ms
DIGITAL I/O: GENERAL						
Output Voltage High (SPIS_MISO)	V_{OH}	I_{SOURCE} = 2mA	V_{DD} - 0.4			V
Output Voltage Low (SPIS_MISO)	V_{OL}	I_{SINK} = 2mA			0.4	V
Input Voltage High (SPIS_SCK, SPIS_SS, SPIS_MOSI)	V_{IH}		0.7 x V_{DD}			V
Input Voltage Low (SPIS_SCK, SPIS_SS, SPIS_MOSI)	V_{IL}				0.3 x V_{DD}	
Input Leakage Current Low	I_{IL}	V_{DD} = 3.63V, V_{IN} = 0V	-500		+500	nA
Input Leakage Current High	I_{IH}	V_{DD} = 3.63V, V_{IN} = 3.63V	-500		+500	nA
SPI SLAVE						
Operating Frequency	f_{SCK}				20	MHz
Clock Period	t_{SCK}			$1/f_{SCK}$		µs
Clock Input High Time	t_{SCH}	(*Note 2*)		$t_{SCK}/2$		µs
Clock Input Low Time	t_{SCL}	(*Note 2*)		$t_{SCK}/2$		µs
SS Active Setup Time	t_{SSE}			10		ns
Data Input Setup Time	t_{SIS}			5		ns
Data Input Hold Time	t_{SIH}			1		ns
Clock Edge to Data Output Valid	t_{SOV}			5		ns
SS Inactive Setup Time	t_{SSD}			10		ns
SS Inactive Time	t_{SSH}			$1/f_{SCK}$		µs
Output Disable Time	t_{SLH}			10		ns
Clock Stable to SS Active	t_{SAD}			10		ns
FLASH MEMORY						
Flash Erase Time	t_{P_ERASE}	Page erase		10		ms
Flash Programming Time per Word	t_{PROG}			8		µs
Flash Endurance	N_{END}		10			kcycles
Data Retention	t_{RET}	T_A = +85°C	10			years

Note 1: System requirement.
Note 2: $t_{SCH} + t_{SCL} \geq 1/f_{SCK}$ (MAX)

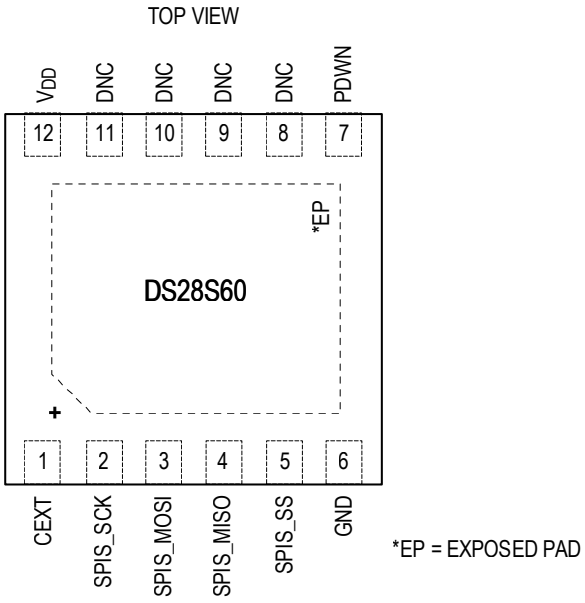
Typical Operating Characteristics

(T_A = T_{MIN} to T_{MAX} unless otherwise noted.)



Pin Configuration

DS28S60



TDFN-EP
3mm x 3mm x 0.75mm

Pin Description

PIN	NAME	FUNCTION
POWER		
1	CEXT	External Capacitor. Connect to ground through a 1µF external ceramic chip capacitor. Place the capacitor as close as possible to the CEXT pin. No other components should be connected to the CEXT pin.
6	GND	Digital Ground. Connect directly to the ground plane.
7	PDWN	Power Down. Controls the power state of the DS28S60. Setting this pin to GND places the DS28S60 into power-down mode. In power-down mode, all volatile/ephemeral registers and data are erased. Set this pin high prior to communicating with the device. This pin should remain in a high state for the duration of any cryptography computations and as long as any ephemeral data/ keys are required by the host application.
12	V_{DD}	Supply Voltage. Connect to the external power supply for the DS28S60. Bypass to ground with a 4.7µF and 0.1µF capacitor in parallel as close as possible to the V_{DD} pin.
—	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.
SPI SLAVE		
2	SPIS_SCK	Slave Clock (SCK). The SPI clock input from an external SPI master controller.
3	SPIS_MOSI	Master Out Slave In (MOSI). This is the SPI data input line from the SPI master.
4	SPIS_MISO	Master In Slave Out (MISO). This is the SPI data output line for data going from the DS28S60 to an external SPI master.
5	SPIS_SS	Slave Select (SS). An input from a SPI master to select the DS28S60 for communication.
8–11	DNC	Do Not Connect. Leave unconnected.

Detailed Description

The DS28S60 secure coprocessor provides a comprehensive cryptographic toolbox, command set, and nonvolatile memory for securing a broad range of embedded equipment. It includes a 3.6KB flash memory array that provides secure storage for keys, certificates, secrets, and application/user data. As a fixed function device, there is no firmware development involved. A simple-to-use command set provides functions and capabilities for:

- Asymmetric key authentication with ECDSA-P256 signature and verification
- Symmetric key authentication with SHA-256 HMAC
- ECDHE secure key exchange
- Encryption/decryption of bulk data with AES-128
- Securely store certificates, keys, and data
- Generation of NIST SP800-90B compliant random data

ChipDNA Physically Unclonable Function (PUF)

ChipDNA PUF security technology provides an exponential increase in protection against the invasive and reverse engineering attacks that hackers apply. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, preventing the discovery of the unique value used by the chip cryptographic functions. Similarly, more exhaustive reverse-engineering attempts are defeated due to the factory conditioning required to make the ChipDNA PUF circuitry operational. The per-device unique key is generated by the ChipDNA PUF circuitry only when needed for cryptographic operations and is then instantaneously deleted.

Most importantly, the ChipDNA secure key never resides statically in registers or memory, nor does it ever leave the electrical boundary of the IC. In addition to the protection benefits, ChipDNA simplifies or eliminates the need for secure IC key management.

Cryptographic Functions

Designed to meet the security requirements of IoT devices, the DS28S60 includes hardware-based cryptographic accelerators. The cryptographic toolbox enables client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery. Segregating the cryptographic functions from the main IoT microcontroller simplifies the overall IoT development effort and ensures that the application level code does not interfere with the security implementation. Typical cryptographic command times are listed in Table 1.

Table 1. Typical Cryptographic Times

CRYPTOGRAPHIC TASK	TIME
ECDSA Computation	t_{OP} x 100
SHA-256 Computation	t_{OP} x 50
AES Computation (Max Data Length)	t_{OP} x 150

Memory

Memory Resources

A secured flash memory array is configured to provide up to 92 pages (32 bytes per page) of programmable user memory. In addition, the flash memory includes reserved pages for keys and secrets. Multiple user-programmable protection modes exist for the user memory space including ECDSA and SHA-256 HMAC R/W authentication protections or optionally left 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.

64-Bit ROM ID

Each DS28S60 contains a unique ROM ID that is 64 bits long. The first 8 bits are a family code. The next 48 bits are a unique serial number. The last 8 bits are a cyclic redundancy check (CRC) of the first 56 bits. See Figure 1 for details.

The CRC is generated using a polynomial generator consisting of a shift register and XOR gates. The polynomial is $X^8 + X^5 + X^4 + 1$. Additional information about the CRC is available in *Application Note 27: Understanding and Using Cyclic Redundancy Checks with Maxim 1-Wire and iButton Products*.

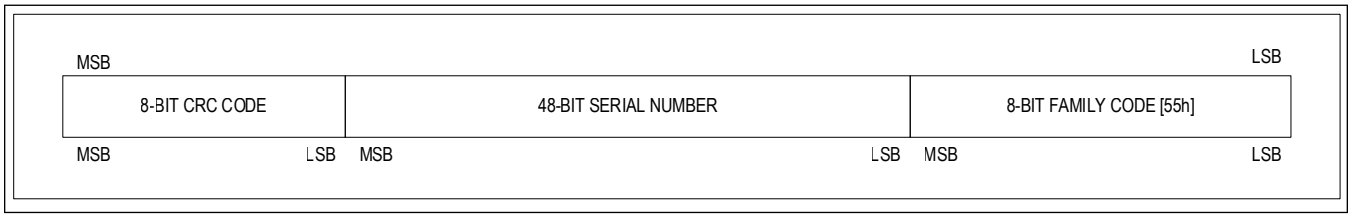


Figure 1. 64-Bit ROM ID

Device Function Commands

After configuring the SPI interface for communication with the DS28S60, a device function command can be transmitted. The data transfer is verified when writing and reading by a CRC of 16-bit type (CRC-16). The CRC-16 is computed as described in *Application Note 27: Understanding and Using Cyclic Redundancy Checks with Maxim 1-Wire and iButton Products*.

Refer to the *DS28S60 Security User Guide* for a list of supported commands. Each command requires a code and one or more parameters. Commands are used to configure, read, write, and perform cryptographic operations. All commands, parameters and data are 8-bit each and require eight serial clock cycles to transmit. The commands, parameters and data are always transferred most significant bit first.

All commands are synchronized to the falling edge of the slave select (SS) input signal. Prior to transmitting a command code, the SPIS_SS signal must be driven low and must remain low until the completion of the command including the command code, the parameters, and all data bits. Any low-to-high transition of the SPIS_SS input prior to completion of the command terminates the in-process command and results in the DS28S60 entering standby mode.

SPI Modes

The DS28S60 supports SPI communications running in either of the following two SPI modes:

- Mode 0 (CPOL = 0, CPHA = 0): Data is sampled at the leading rising edge of the clock.
- Mode 3 (CPOL = 1, CPHA =1): Data is sampled on the trailing rising edge of the clock.

Details of the timing are described in Figure 2.

If enabled, an autodetect feature is available to detect between Mode 0 and Mode 3. The feature works by checking if the SPIS_SCK signal is low (Mode 0) or high (Mode 3) before the falling edge of the SPIS_SS signal during the t_{SAD} time. Mode 1 and Mode 2 are not supported.

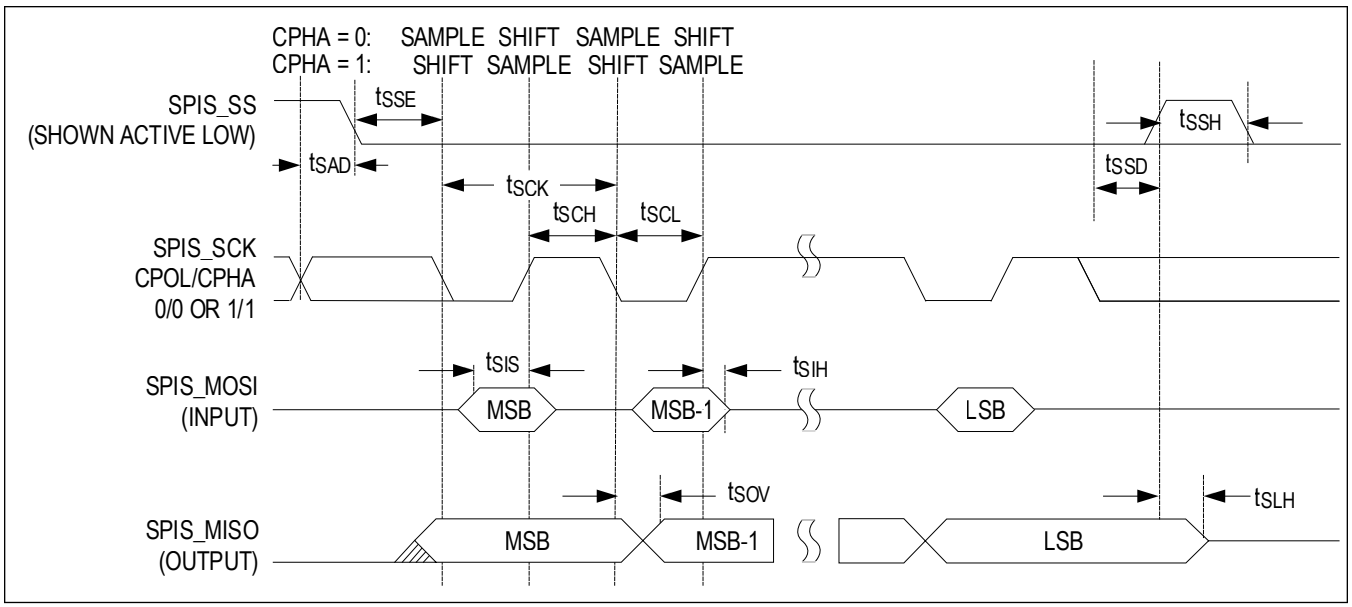
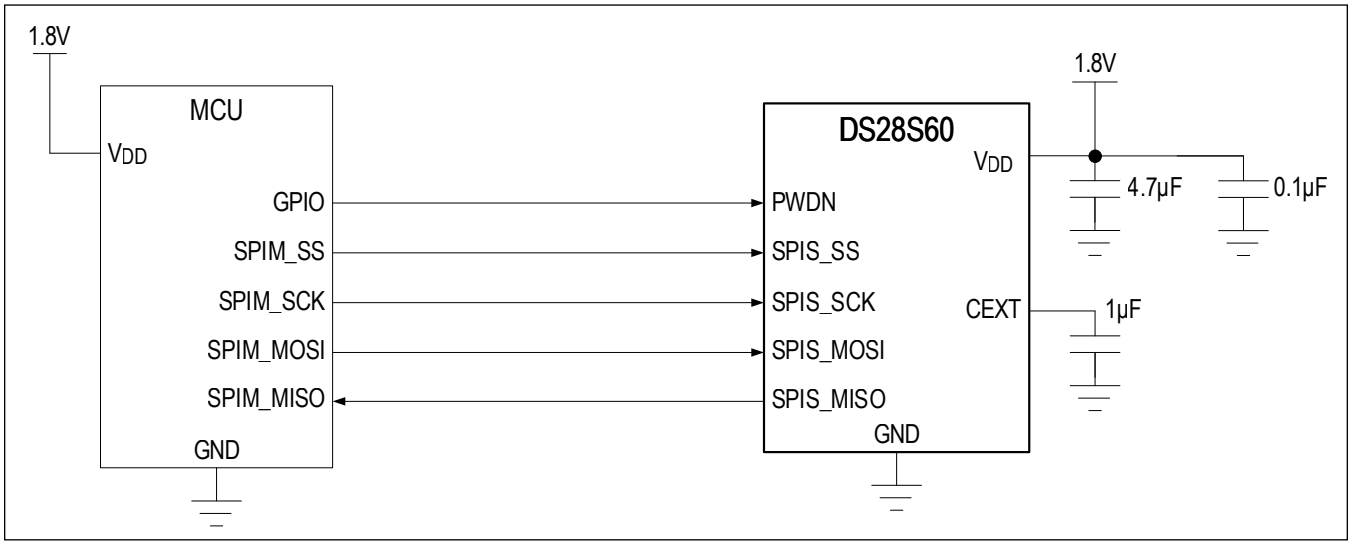


Figure 2. SPI Mode 0 and 3 Data Sampling Edges

Typical Application Circuit

Simple Application-Level Diagram



Ordering Information

PART NUMBER	USER FLASH MEMORY	TEMP RANGE	PIN-PACKAGE
DS28S60Q+	3.6KB	-40°C to +105°C	12 TDFN

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