Click here for production status of specific part numbers.

MAX32520

ChipDNA Secure Arm Cortex M4 Microcontroller

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 microcontroller MAX32520 provides an interoperable, secure, and cost-effective solution to build new generations of trusted embedded systems and communication devices such as IoT, IoT gateways, and wireless access points.

The MAX32520 incorporates Maxim's patented ChipDNA™ PUF technology. ChipDNA technology involves a physically unclonable function (PUF) that enables cost-effective protection against invasive physical 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 cryptographic functions. The MAX32520 utilizes the ChipDNA output as key content to cryptographically secure all device stored data including user firmware. User firmware encryption provides ultimate software IP protection. The ChipDNA can also generate a private key for the ECDSA signing operation.

The MAX32520 integrates an Arm® Cortex® -M4 processor, 2MB of Flash, 136KB of system RAM + 34KB ECC, 8KB of one-time-programmable (OTP) memory and 128KB of boot ROM.

The MAX32520 provides a FIPS/NIST compliant TRNG, environmental and tamper detection circuitry to facilitate system-level security.

Multiple high-speed interfaces are supported including SPI, UART, and an I^2C. The four on-chip timers also support PWM output generation for direct control of external devices. One of the SPI ports has a serial flash emulation mode allowing direct code fetching enabling secure boot for a host microcontroller.

Applications

- Embedded Connected Systems
- Secure Industrial Appliances, Sensors, and Controllers
- IoT Nodes and Gateways
- Embedded Communication Equipment (Routers, Gateways, etc.)
- Set-Top Boxes

Benefits and Features

- High-Efficiency Microcontroller for Secure Element IoT
  - Arm Cortex-M4F with FPU Up to 120MHz
  - 16KB Unified Code Cache
  - 2MB PUF Encrypted Flash Memory with Cache Provides Ultimate Firmware IP Protection
  - Low Latency On-the-Fly Decryption of Flash Execution
  - 136KB SRAM + 34KB ECC
  - 8KB User-Programmable OTP
- Secure Element
  - PUF-Based Keys
    - For Internal Flash Encryption
    - For Strong Device Authentication
  - Secure Boot Loader with Public Key Authentication and Serial Flash Emulation
  - AES, SHA, and ECDSA Accelerators
  - Hardware True Random Number Generator
    - SP800-90B Compliant Entropy Source
    - SP800-90A Compliant DRBG
  - Die Shield
  - Temperature and Voltage Tamper Monitor
  - External Tamper Sensor with Random Dynamic Pattern
- Power Management Maximizes Operating Time for Battery Applications
  - Single 3.3V/2.5V/1.8V Supply
  - Down to 3.2µA Backup Mode
  - 15µs Wake-Up Time from Standby Mode
  - Clock Gating, Power Gating, Registers, and Memory Retention Modes
- Multiple Peripherals for System Control
  - One UART
  - One I^2C Interface
  - QSPI
  - Four Timers with PWM Capability
  - Up to 27 General-Purpose I/O Pins with Selectable Output Driver Strength
  - 4-Channel DMA Controller
  - 4-Pin JTAG

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

19-100583; Rev 0; 6/19

Simplified Block Diagram

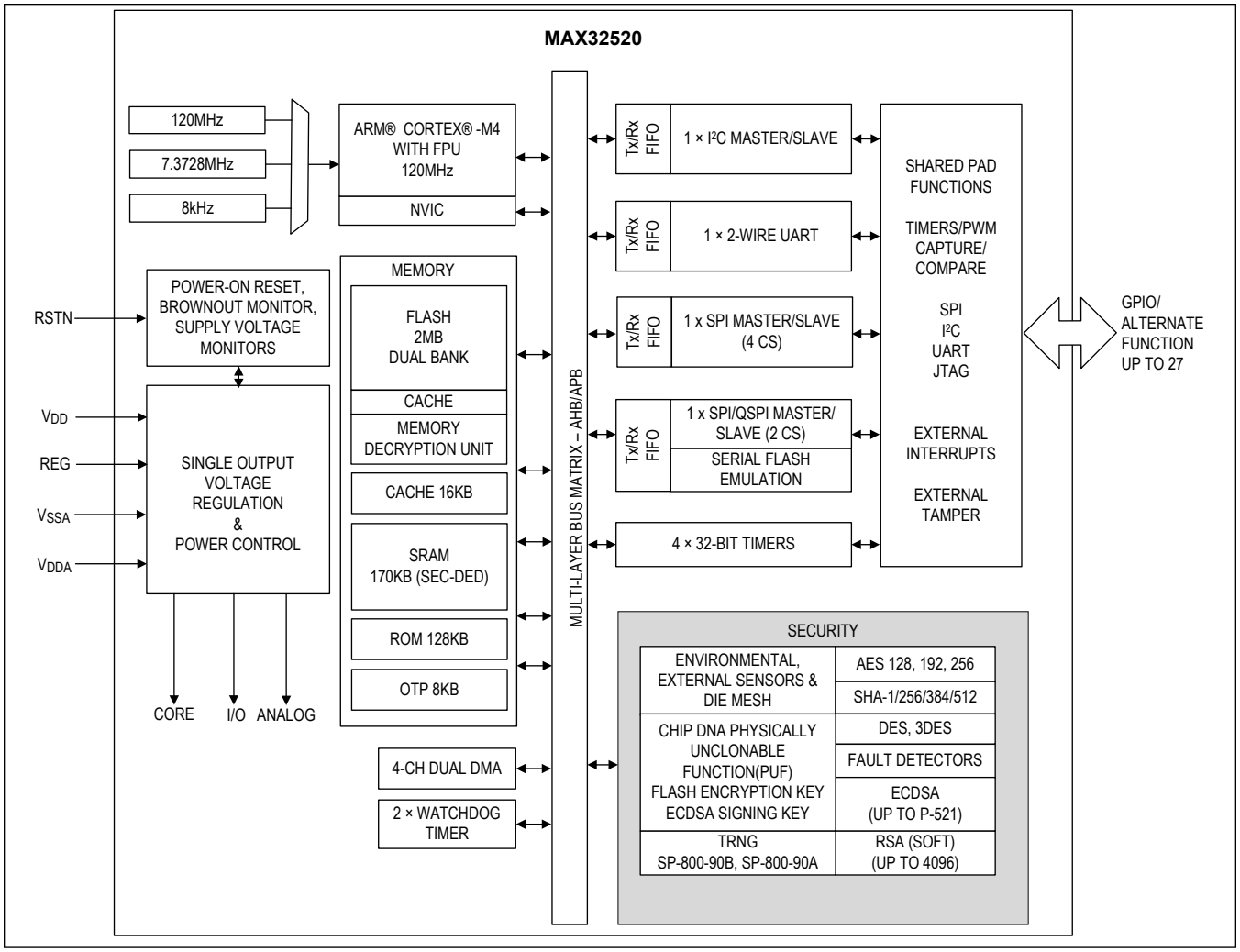


TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

LIST OF FIGURES

LIST OF TABLES

Absolute Maximum Ratings

Continuous Power Dissipation (T_A = +70°C) (Single-layer board, derate 21.3mW/°C above +70°C)..... 1702.1mW
Continuous Power Dissipation TQFN (Multilayer Board) (T_A = +70°C, derate 34.5mW/°C above +70°C.)..... 2758.6 mW
Operating Temperature Range ..... -40°C to +105°C
Storage Temperature Range..... -65°C to +150°C
V_{DD}..... -0.3V to 3.6V
V_{DDA}..... -0.3V to 3.6V
RSTN, GPIO ..... -0.3V to V_{DD} + 0.5V
V_{SSA} 1mA
V_{SS} 100mA
Output Current (sink) by Any GPIO Pin 25mA
Output Current (source) by Any GPIO Pin..... -25mA

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

32 TQFN

Package Code	T3255+8C
Outline Number	21-0140
Land Pattern Number	90-0013
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	47°C/W
Junction to Case (θ_{JC})	1.70°C/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	29°C/W
Junction to Case (θ_{JC})	1.70°C/W

30 WLP

Package Code	W302N2+1
Outline Number	21-100380
Land Pattern Number	Refer to Application Note 1891
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	49.38°C/W
Junction to Case (θ_{JC})	N/A

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 and T_A = +105°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.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
POWER SUPPLIES						
Input Supply Voltage, Digital	V_{DD}		1.71	1.8	3.6	V
Input Supply Voltage, Analog	V_{DDA}		1.71	1.8	3.6	V

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25°C and T_A = +105°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.)

PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
V_{DD} Current, Active Mode	I_{DD_ACT}	Total current into V_{DD} pins, f_{SYS_CLK} = 120MHz, CPU in Active mode, executing While(1) from cache, inputs tied to V_{SS}, outputs source/sink 0mA	V_{DD} = 1.8V		10.6		mA
			V_{DD} = 3.3V		10.7		
V_{DD} Current, Sleep Mode	I_{DD_SLP}	Total current into V_{DD} pins, f_{SYS_CLK} = 120MHz, CPU in Sleep mode, inputs tied to V_{SS}, outputs source/sink 0mA	V_{DD} = 1.8V		2.16		mA
			V_{DD} = 3.3V		2.35		
V_{DD} Fixed Current, DeepSleep Mode	I_{DD_FDSL}	Standby state with full retention	V_{DD} = 1.8V		65		µA
			V_{DD} = 3.3V		69		
V_{DD} Current, Backup Mode	I_{DD_BK}	Total current into V_{DD} pins, inputs tied to V_{SS}, AES keys retained, outputs source/sink 0mA	72KB ECC memory retention, V_{DD} = 1.8V		4.72		µA
			72KB ECC memory retention, V_{DD} = 3.3V		6.74		
			No memory retention, V_{DD} = 1.8V		3.22		
			No memory retention, V_{DD} = 3.3V		5.25		
			32KB ECC memory retention, V_{DD} = 1.8V		3.84		
			32KB ECC memory retention, V_{DD} = 3.3V		5.87		
			64KB ECC memory retention, V_{DD} = 1.8V		4.4		
			64KB ECC memory retention, V_{DD} = 3.3V		6.5		
CLOCKS							
System Clock Frequency	f_{SYS_CLK}			0.0625		120,000	kHz

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25°C and T_A = +105°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.)

PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
System Clock Period	t_{SYS_CLK}				1/ f_{SYS_CLK}		ns
Nano-ring Oscillator Frequency	f_{NANO}				8		kHz
High-Speed Oscillator Frequency	f_{HSCLK}			115.5	120	124.5	MHz
7MHz Oscillator Frequency	f_{7MCLK}				7.3728		MHz
GENERAL-PURPOSE I/O							
Input Low Voltage for All GPIO	V_{IL}					0.3 x V_{DD}	V
Input Low Voltage for RSTN	V_{IL_RSTN}					0.3 x V_{DD}	V
Input High Voltage for All GPIO	V_{IH}			0.7 x V_{DD}			V
Input High Voltage for RSTN	V_{IH_RSTN}			0.7 x V_{DD}			V
Output Low Voltage for All GPIO	V_{OL}	V_{DD} = 1.71V	GPIOn_DS_SEL[1:0] = 00, I_{OL} = 1mA		0.2	0.4	V
			GPIOn_DS_SEL[1:0] = 01, I_{OL} = 2mA		0.2	0.4	
			GPIOn_DS_SEL[1:0] = 10, I_{OL} = 4mA		0.2	0.4	
			GPIOn_DS_SEL[1:0] = 11, I_{OL} = 8mA		0.2	0.4	
Combined I_{OL}, All GPIO	I_{OL_TOTAL}	GBD				48	mA
Output High Voltage for All GPIO	V_{OH}	V_{DD} = 1.71V	GPIOn_DS_SEL[1:0] = 00, I_{OL} = -1mA	V_{DD} - 0.4			V
			GPIOn_DS_SEL[1:0] = 01, I_{OL} = -2mA	V_{DD} - 0.4			
			GPIOn_DS_SEL[1:0] = 10, I_{OL} = -4mA	V_{DD} - 0.4			
			GPIOn_DS_SEL[1:0] = 11, I_{OL} = -8mA	V_{DD} - 0.4			
Combined I_{OH}, All GPIO	I_{OH_TOTAL}	GBD				-48	mA
Input Hysteresis (Schmitt)	V_{IHYS}				300		mV
Input Leakage Current Low	I_{IL}	V_{DD} = 3.6V, V_{IN} = 0V, internal pullup disabled		-1		+1	µA
Input Leakage Current High	I_{IH}	V_{DD} = 3.6V, V_{IN} = 3.6V, internal pulldown disabled		-1		+1	µA

Electrical Characteristics (continued)

(Limits are 100% tested at T_A = +25°C and T_A = +105°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.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Input Pullup Resistor RSTN	R_{PU_R}			25		kΩ
Input Pullup/Pulldown Resistor for All GPIO	R_{PU1}	Normal resistance		25		kΩ
	R_{PU2}	Highest resistance		1		MΩ
ENVIRONMENTAL SENSORS						
V_{DD} Overvoltage Threshold	V_{DD_OV}		3.6		3.8	V
V_{DD} Undervoltage Threshold	V_{DD_UV}	VTM_LOTHSEL = [00]	1.56	1.66	1.76	V
		VTM_LOTHSEL = [01]	2.1	2.2	2.3	
		VTM_LOTHSEL = [1x]	2.7	2.8	2.9	
High-Temperature Threshold	T_{HTR}	GBD	115	125	135	°C
Low-Temperature Threshold	T_{LTR1}	GBD	-70	-60	-50	°C
	T_{LTR2}	GBD	-50	-40	-30	

Electrical Characteristics—SPI

(Timing specifications are guaranteed by design and not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
MASTER MODE						
SPI Master Operating Frequency	f_{MCK}	f_{SYS_CLK} = 120MHz, $f_{MCK(MAX)}$ = $f_{SYS\_CLK}/2$			60	MHz
SPI Master SCK Period	t_{MCK}			$1/f_{MCK}$		ns
SCK Output Pulse-Width High/Low	t_{MCH}, t_{MCL}		$t_{MCK}/2$			ns
MOSI Output Hold Time After SCK Sample Edge	t_{MOH}		$t_{MCK}/2$			ns
MOSI Output Valid to Sample Edge	t_{MOV}		$t_{MCK}/2$			ns
MOSI Output Hold Time After SCK Low Idle	t_{MLH}			$t_{MCK}/2$		ns
MISO Input Valid to SCK Sample Edge Setup	t_{MIS}			5		ns
MISO Input to SCK Sample Edge Hold	t_{MIH}			$t_{MCK}/2$		ns
SLAVE MODE						
SPI Slave Operating Frequency	f_{SCK}				50	MHz
SPI Slave SCK Period	t_{SCK}			$1/f_{SCK}$		ns
SCK Input Pulse-Width High/Low	t_{SCH}, t_{SCL}			$t_{SCK}/2$		

Electrical Characteristics—SPI (continued)

(Timing specifications are guaranteed by design and not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SSx Active to First Shift Edge	t_{SSE}			10		ns
MOSI Input to SCK Sample Edge Rise/Fall Setup	t_{SIS}			5		ns
MOSI Input from SCK Sample Edge Transition Hold	t_{SIH}			1		ns
MISO Output Valid After SCLK Shift Edge Transition	t_{SOV}			5		ns
SCK Inactive to SSx Inactive	t_{SSD}			10		ns
SSx Inactive Time	t_{SSH}			$1/f_{SCK}$		µs
MISO Hold Time After SSx Deassertion	t_{SLH}			10		ns

Electrical Characteristics—I^2C

(TIming specifications are guaranteed by design and not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
STANDARD MODE						
Output Fall Time	t_{OF}	Standard mode, from $V_{IH(MIN)}$ to $V_{IL(MAX)}$		150		ns
SCL Clock Frequency	f_{SCL}		0		100	kHz
Low Period SCL Clock	t_{LOW}		4.7			µs
High Time SCL Clock	t_{HIGH}		4.0			µs
Setup Time for Repeated Start Condition	$t_{SU;STA}$		4.7			µs
Hold Time for Repeated Start Condition	$t_{HD;STA}$		4.0			µs
Data Setup Time	$t_{SU;DAT}$			300		ns
Data Hold Time	$t_{HD;DAT}$			10		ns
Rise Time for SDA and SCL	t_R			800		ns
Fall Time for SDA and SCL	t_F			200		ns
Setup Time for a Stop Condition	$t_{SU;STO}$		4.0			µs
Bus Free Time Between a Stop and Start Condition	t_{BUS}		4.7			µs
Data Valid Time	$t_{VD;DAT}$		3.45			µs

Electrical Characteristics—I²C (continued)

(TIming specifications are guaranteed by design and not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Data Valid Acknowledge Time	$t_{VD;ACK}$		3.45			µs
FAST MODE						
Output Fall Time	t_{OF}	From $V_{IH(MIN)}$ to $V_{IL(MAX)}$		150		ns
Pulse Width Suppressed by Input Filter	t_{SP}			75		ns
SCL Clock Frequency	f_{SCL}		0		400	kHz
Low Period SCL Clock	t_{LOW}		1.3			µs
High Time SCL Clock	t_{HIGH}		0.6			µs
Setup Time for Repeated Start Condition	$t_{SU;STA}$		0.6			µs
Hold Time for Repeated Start Condition	$t_{HD;STA}$		0.6			µs
Data Setup Time	$t_{SU;DAT}$			125		ns
Data Hold Time	$t_{HD;DAT}$			10		ns
Rise Time for SDA and SCL	t_R			30		ns
Fall Time for SDA and SCL	t_F			30		ns
Setup Time for a Stop Condition	$t_{SU;STO}$		0.6			µs
Bus Free Time Between a Stop and Start Condition	t_{BUS}		1.3			µs
Data Valid Time	$t_{VD;DAT}$		0.9			µs
Data Valid Acknowledge Time	$t_{VD;ACK}$		0.9			µs
FAST MODE PLUS						
Output Fall Time	t_{OF}	From $V_{IH(MIN)}$ to $V_{IL(MAX)}$		80		ns
Pulse Width Suppressed by Input Filter	t_{SP}			75		ns
SCL Clock Frequency	f_{SCL}		0		1000	kHz
Low Period SCL Clock	t_{LOW}		0.5			µs
High Time SCL clock	t_{HIGH}		0.26			µs
Setup Time for Repeated Start Condition	$t_{SU;STA}$		0.26			µs
Hold Time for Repeated Start Condition	$t_{HD;STA}$		0.26			µs
Data Setup Time	$t_{SU;DAT}$			50		ns
Data Hold Time	$t_{HD;DAT}$			10		ns

Electrical Characteristics—I²C (continued)

(TIming specifications are guaranteed by design and not production tested.)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Rise Time for SDA and SCL	t_R			50		ns
Fall Time for SDA and SCL	t_F			30		ns
Setup Time for a Stop Condition	$t_{SU;STO}$		0.26			µs
Bus Free Time Between a Stop and Start Condition	t_{BUS}		0.5			µs
Data Valid Time	$t_{VD;DAT}$		0.45			µs
Data Valid Acknowledge Time	$t_{VD;ACK}$		0.45			µs

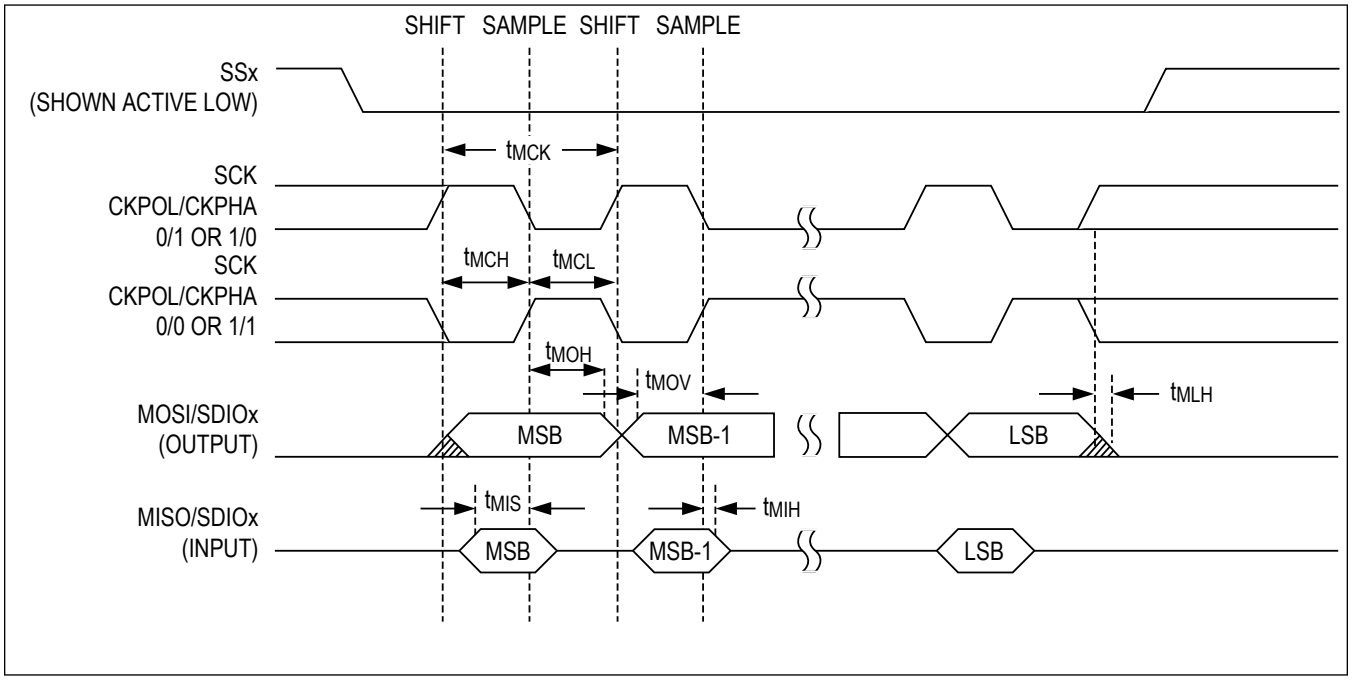


Figure 1. SPI Master Mode Timing Diagram

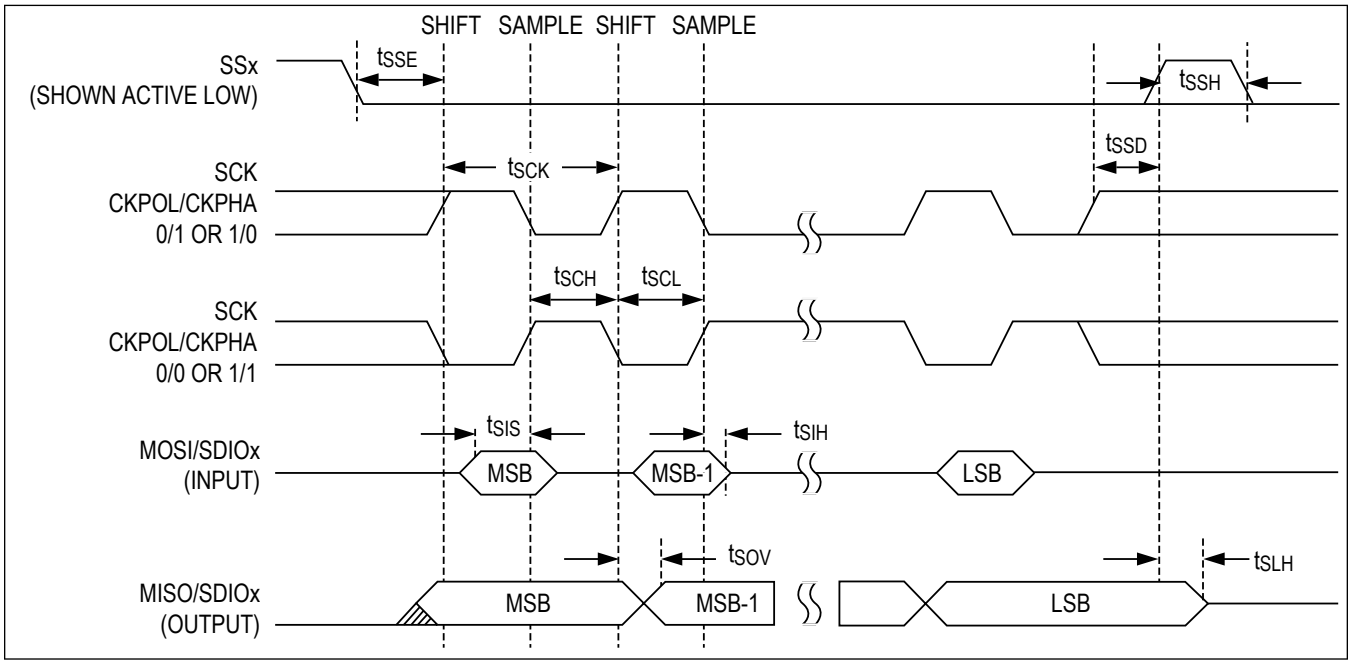


Figure 2. SPI Slave Mode Timing Diagram

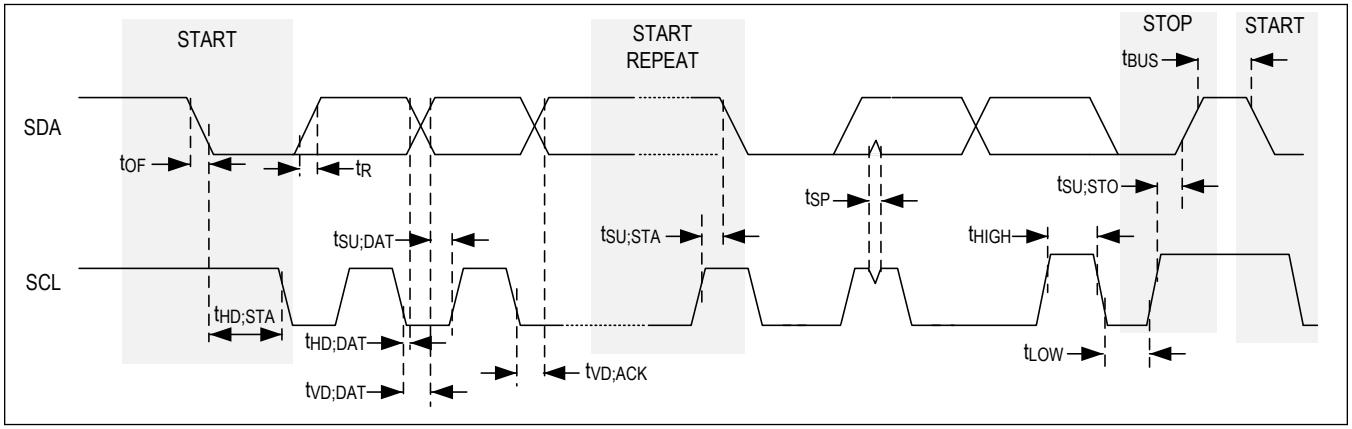
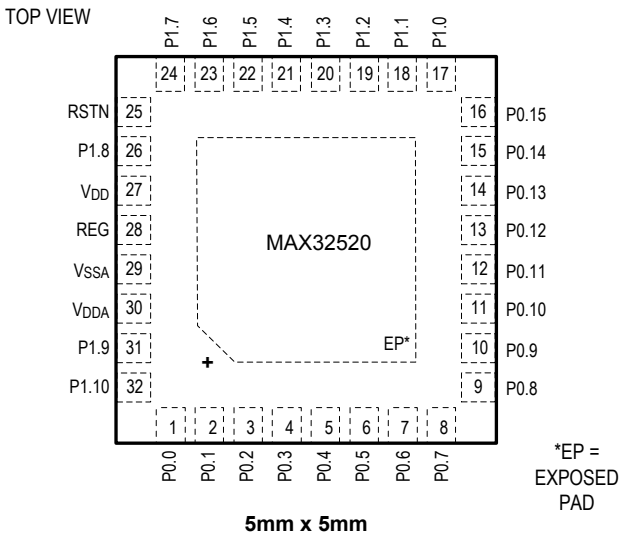


Figure 3. I^2C Timing Diagram

Pin Configuration

32 TQFN



Pin Description

PIN	NAME	FUNCTION MODE			FUNCTION
		Primary Signal (Default)	Alternate Function 1	Alternate Function 2	
UART					
1	P0.0	P0.0	UART_RXD	—	P0.0: GPIO0 Port 0 UART_RXD: UART Data Input
2	P0.1	P0.1	UART_TXD	—	P0.1: GPIO1 Port 0 UART_TXD: UART Data Output
SPI					
3	P0.2	P0.2	SPI0_DIO0 (MOSI0)	SFSPIS_DIO0 (SFSI)	P0.2: GPIO2 Port 0 SPI0_DIO0: Quad SPI I/O 0 (SPI0 Master Out Slave In) SFSPIS_DIO0: Serial Flash SPI Slave I/O 0 (SFSPI Slave In)
4	P0.3	P0.3	SPI0_DIO1 (MISO0)	SFSPIS_DIO1 (SFSO)	P0.3: GPIO3 Port 0 SPI0_DIO1: Quad SPI I/O 1 (SPI0 Master In Slave Out) SFSPIS_DIO1: Serial Flash SPI I/O 1 (SFSPI Slave Out)
5	P0.4	P0.4	SCK0	SFSPIS_SCK	P0.4: GPIO4 Port 0 SCK0: SPI0 Clock SFSPIS_SCK: Serial Flash SPI Clock
6	P0.5	P0.5	SSEL0_0	SFSPIS_SS0	P0.5: GPIO5 Port 0 SSEL0_0: SPI0 Slave Select 0 SFSPIS_SS0: Serial Flash SPI Slave Select 0

32 TQFN

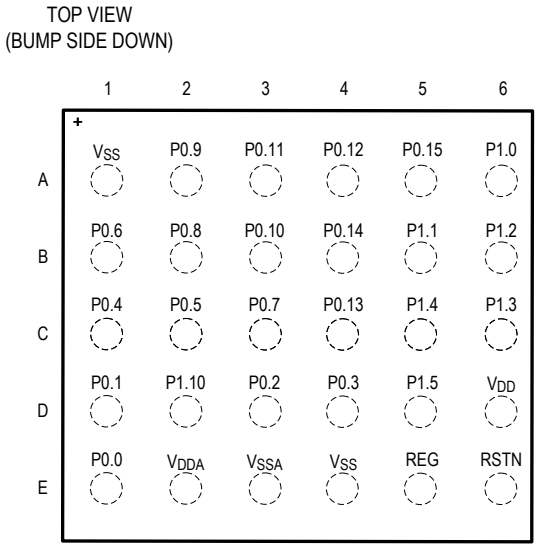
PIN	NAME	FUNCTION MODE			FUNCTION
		Primary Signal (Default)	Alternate Function 1	Alternate Function 2	
7	P0.6	P0.6	SSEL0_1	SFSPIS_SS1	P0.6: GPIO6 Port 0 SSEL0_1: SPI0 Slave Select 1 SFSPIS_SS1: Serial Flash SPI Slave Select 1
8	P0.7	P0.7	SPI0_DIO2	SFSPIS_DIO2	P0.7: GPIO7 Port 0 SPI0_DIO2: Quad SPI I/O 2 SFSPIS_DIO2: Serial Flash SPI I/O 2
9	P0.8	P0.8	SPI0_DIO3	SFSPIS_DIO3	P0.8: GPIO8 Port 0 SPI0_DIO3: Quad SPI I/O3 SFSPIS_DIO3: Serial Flash SPI I/O 3
12	P0.11	P0.11	MISO1	—	P0.11: GPIO11 Port 0 MISO1: SPI1 Master In Slave Out
13	P0.12	P0.12	MOSI1	—	P0.12: GPIO12 Port 0 MOSI1: SPI1 Master Out Slave In
14	P0.13	P0.13	SCK1	—	P0.13: GPIO13 Port 0 SCK1: SPI1 Clock
15	P0.14	P0.14	SSEL1_0	—	P0.14: GPIO14 Port 0 SSEL1_0: SPI1 Slave Select 0
16	P0.15	P0.15	SSEL1_1	—	P0.15: GPIO15 Port 0 SSEL1_1: SPI1 Slave Select 1
I²C					
10	P0.9	P0.9	SDA	—	P0.9: GPIO9 Port 0 SDA: I2C Data
11	P0.10	P0.10	SCL	—	P0.10: GPIO10 Port 0 SCL: I2C Clock
TIMER					
17	P1.0	P1.0	TCLK0	—	P1.0: GPIO0 Port 1 TCLK0: Timer 0 Clock I/O
18	P1.1	P1.1	TCLK1	—	P1.1: GPIO1 Port 1 TCLK1: Timer 1 Clock I/O
23	P1.6	P1.6	TCLK2	SSEL1_2	P1.6: GPIO6 Port 1 TCLK2: Timer 2 Clock I/O SSEL1_2: SPI1 Slave Select 2
24	P1.7	P1.7	TCLK3	SSEL1_3	P1.7: GPIO7 Port 1 TCLK3: Timer 3 Clock I/O SSEL1_3: SPI1 Slave Select 3
JTAG					
19	P1.2	P1.2	TDI	—	P1.2: GPIO2 Port 1 TDI: JTAG Test Data Input
20	P1.3	P1.3	TDO	—	P1.3: GPIO3 Port 1 TDO: JTAG Test Data Output
21	P1.4	P1.4	TMS/SWDIO	—	P1.4: GPIO4 Port 1 TMS/SWDIO: JTAG Mode Select / Single Wire Debug I/O

32 TQFN

PIN	NAME	FUNCTION MODE			FUNCTION
		Primary Signal (Default)	Alternate Function 1	Alternate Function 2	
22	P1.5	P1.5	TCK/SWCLK	—	P1.5: GPIO5 Port 1 TCK/SWCLK: JTAG Test Clock / Single Wire Debug Clock
EXTERNAL TAMPER					
26	P1.8	P1.8	EXT_SENS_OUT	—	P1.8: GPIO8 Port 1 EXT_SENS_OUT: External Sensor Output
31	P1.9	P1.9	EXT_SENS_IN	—	P1.9: GPIO9 Port 1 EXT_SENS_IN: External Sensor Input
32	P1.10	P1.10	TAMPER_OUT	—	P1.10: GPIO10 Port 1 TAMPER_OUT: External Tamper Detection Output. This pin is active when external tamper is detected.
POWER AND SYSTEM					
27	V_{DD}	V_{DD}	—	—	V_{DD}: Core and I/O supply voltage. Bypass V_{DD} with 1µf and 100nF capacitors with ESR <100mΩ
28	REG	REG	—	—	REG: Regulator Capacitor. Bypass REG with 1µf and 100nF capacitors with ESR < 100mΩ
29	V_{SSA}	V_{SSA}	—	—	V_{SSA}: 1.8V Analog Ground
30	V_{DDA}	V_{DDA}	—	—	V_{DDA}: 1.8V Analog Power Supply. Bypass V_{DDA} with 1µf and 100nF capacitors with ESR < 100mΩ
—	EP	V_{SS}	—	—	Exposed Pad. Ground.
25	RSTN	RSTN	—	—	RSTN: Hardware Reset (Active-Low) Input. The device remains in reset while this pin is in its active state. When the pin transitions to its inactive state, the device performs a warm reset (resetting all logic) and begins execution. This pin has an internal pullup to the V_{DD} supply. This pin should be left unconnected if the system design does not provide a reset signal to the device.

Pin Configuration

30 WLP



2.6mm x 2.6mm

Pin Description

PIN	NAME	FUNCTION MODE			FUNCTION
		Primary Signal (Default)	Alternate Function 1	Alternate Function 2	
UART					
E1	P0.0	P0.0	UART_RXD	—	P0.0: GPIO0 Port 0 UART_RXD: UART Data Input
D1	P0.1	P0.1	UART_TXD	—	P0.1: GPIO1 Port 0 UART_TXD: UART Data Output
SPI					
D3	P0.2	P0.2	SPI0_DIO0 (MOSI0)	SFSPIS_DIO0 (SFSI)	P0.2: GPIO2 Port 0 SPI0_DIO0: Quad SPI I/O 0 (SPI0 Master Out Slave In) SFSPIS_DIO0: Serial Flash SPI Slave I/O 0 (SFSPI Slave In)
D4	P0.3	P0.3	SPI0_DIO1 (MISO0)	SFSPIS_DIO1 (SFSO)	P0.3: GPIO3 Port 0 SPI0_DIO1: Quad SPI I/O 1 (SPI0 Master In Slave Out) SFSPIS_DIO1: Serial Flash SPI I/O 1 (SFSPI Slave Out)
C1	P0.4	P0.4	SCK0	SFSPIS_SCK	P0.4: GPIO4 Port 0 SCK0: SPI0 Clock SFSPIS_SCK: Serial SPI Clock

30 WLP

PIN	NAME	FUNCTION MODE			FUNCTION
		Primary Signal (Default)	Alternate Function 1	Alternate Function 2	
C2	P0.5	P0.5	SSEL0_0	SFSPIS_SS0	P0.5: GPIO5 Port 0 SSEL0_0: SPI0 Slave Select 0 SFSPIS_SS0: Serial Flash SPI Slave Select 0
B1	P0.6	P0.6	SSEL0_1	SFSPIS_SS1	P0.6: GPIO6 Port 0 SSEL0_1: SPI0 Slave Select 1 SFSPIS_SS1: Serial Flash SPI Slave Select 1
C3	P0.7	P0.7	SPI0_DIO2	SFSPIS_DIO2	P0.7: GPIO7 Port 0 SPI0_DIO2: Quad SPI I/O 2 SFSPIS_DIO2: Serial Flash SPI I/O 2
B2	P0.8	P0.8	SPI0_DIO3	SFSPIS_DIO3	P0.8: GPIO8 Port 0 SPI0_DIO3: Quad SPI I/O3 SFSPIS_DIO3: Serial Flash SPI I/O 3
A3	P0.11	P0.11	MISO1	—	P0.11: GPIO11 Port 0 MISO1: SPI1 Master In Slave Out
A4	P0.12	P0.12	MOSI1	—	P0.12: GPIO12 Port 0 MOSI1: SPI1 Master Out Slave In
C4	P0.13	P0.13	SCK1	—	P0.13: GPIO13 Port 0 SCK1: SPI1 Clock
B4	P0.14	P0.14	SSEL1_0	—	P0.14: GPIO14 Port 0 SSEL1_0: SPI1 Slave Select 0
A5	P0.15	P0.15	SSEL1_1	—	P0.15: GPIO15 Port 0 SSEL1_1: SPI1 Slave Select 1
I²C					
A2	P0.9	P0.9	SDA	—	P0.9: GPIO9 Port 0 SDA: I2C Data
B3	P0.10	P0.10	SCL	—	P0.10: GPIO10 Port 0 SCL: I2C Clock
TIMER					
A6	P1.0	P1.0	TCLK0	—	P1.0: GPIO0 Port1 TCLK0: Timer 0 Clock I/O
B5	P1.1	P1.1	TCLK1	—	P1.1: GPIO1 Port1 TCLK1: Timer 1 Clock I/O
JTAG					
B6	P1.2	P1.2	TDI	—	P1.2: GPIO2 Port 1 TDI: JTAG Test Data Input
C6	P1.3	P1.3	TDO	—	P1.3: GPIO3 Port 1 TDO: JTAG Test Data Output
C5	P1.4	P1.4	TMS/SWDIO	—	P1.4: GPIO4 Port 1 TMS/SWDIO: JTAG Mode Select / Single Wire Debug I/O
D5	P1.5	P1.5	TCK/SWCLK	—	P1.5: GPIO5 Port 1 TCK/SWCLK: JTAG Test Clock / Single Wire Debug Clock

30 WLP

PIN	NAME	FUNCTION MODE			FUNCTION
		Primary Signal (Default)	Alternate Function 1	Alternate Function 2	
POWER AND SYSTEM					
D6	V_{DD}	V_{DD}	—	—	V_{DD}: Core and I/O Supply Voltage. Bypass V_{DD} with 1µf and 100nF capacitors with ESR < 100mΩ.
E5	REG	REG	—	—	REG: Regulator Capacitor. Bypass REG with 1µf and 100nF capacitors with ESR < 100mΩ.
E3	V_{SSA}	V_{SSA}	—	—	V_{SSA}: 1.8V Analog Ground
E2	V_{DDA}	V_{DDA}	—	—	V_{DDA}: 1.8V Analog Power Supply. Bypass V_{DDA} with 1µf and 100nF capacitors with ESR < 100mΩ.
E4, A1	V_{SS}	V_{SS}	—	—	Ground
E6	RSTN	RSTN	—	—	RSTN: Hardware Reset (Active-Low) Input. The device remains in reset while this pin is in its active state. When the pin transitions to its inactive state, the device performs a warm reset (resetting all logic) and begins execution. This pin has an internal pullup to the V_{DD} supply. This pin should be left unconnected if the system design does not provide a reset signal to the device.
D2	P1.10	P1.10	TAMPER_OUT	—	P1.10: GPIO10 Port 1 TAMPER_OUT: External Tamper Detection Output. This pin is active when external tamper is detected.

Detailed 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 microcontroller MAX32520 provides an interoperable, secure, and cost-effective solution to build new generations of trusted embedded systems and communication devices such as wireless access points. The MAX32520 incorporates Maxim's patented ChipDNA™ PUF technology. ChipDNA technology involves a physically unclonable function (PUF) that enables cost-effective protection against invasive physical 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 to prevent the discovery of the unique value used by the chip cryptographic functions. The MAX32520 utilizes the ChipDNA output as key content to cryptographically secure all device stored data and optionally, under user control, as the private key for the ECDSA signing operation. The MAX32520 integrates an Arm Cortex-M4 processor, 2MB of flash, 136KB of system RAM + 34KB ECC, 8KB of one-time-programmable (OTP) memory and 128KB of boot ROM.

In addition to hardware crypto functions, the MAX32520 provides a FIPS/NIST-compliant true random number generator, as well as environmental and tamper detection circuitry to facilitate system-level security for the application.

The MAX32520 microcontroller includes multiple communication interfaces: two SPI ports, one UART, and an I^2C bus. The four on-chip timers also support PWM output generation for direct control of external devices. One of the SPI ports has a serial flash emulation mode to allow direct code fetching and thus enable a secure boot for a host microcontroller.

Arm Cortex-M4 with FPU Processor

The Arm Cortex-M4 with FPU processor combines high-efficiency signal processing functionality with flexible low-power operating modes. The features of this implementation of the familiar Arm Cortex-M4 architecture include:

- Floating point unit (FPU)
- Memory protection unit
- Full debug support level
  - Debug access port (DAP)
  - Breakpoints
  - Flash patch
  - Halting debug
  - Development and debug interface
- NVIC support
  - Programmable IRQ generation for each interrupt source
  - Unique vectors for each interrupt channel
  - 8 programmable priority levels support nesting and preemption
  - External GPIO interrupts grouped by GPIO port
- DSP supports single instruction multiple data (SIMD) path DSP extensions, providing:
  - 4 parallel 8-bit add/sub
  - 2 parallel 16-bit add/sub
  - 2 parallel MACs
  - 32- or 64-bit accumulate
  - Signed, unsigned, data with or without saturation

Memory

Internal Flash Memory

2MB of internal flash memory provides nonvolatile storage of program and data memory. The flash memory can be fully AES encrypted using a 256-bit, PUF-generated key. In this case, the memory content is decrypted on the fly for execution. Firmware encryption through AES- and PUF-generated encryption key provides unmatched level of software

IP protection.

A dedicated state machine enables direct access to the flash block. Thanks to this state machine the MAX32520 can emulate a serial flash and the content of the flash is directly accessible from a host CPU. The typical application is the support of the secure boot function for a host processor.

Internal SRAM

The internal 170KB SRAM provides low-power retention of application information in all power modes except shutdown. The SRAM can be configured as 136KB + 34KB ECC SEC-DED.

The internal SRAM can be divided into granular banks that create a flexible SRAM retention architecture. This data retention feature is optional and configurable. This granularity allows the application to minimize its power consumption by only retaining the most essential data.

Internal ROM and Boot Loader

Upon assertion and deassertion of system reset, the Arm Cortex-M4 is reset and begins program execution of internal ROM code. A secure bootloader is implemented to provide trusted boot, secure flash upload, and flash integrity verification upon reboot.

A built-in public key authentication scheme allows secure firmware updates from both UART and SPI interfaces.

Clocking Scheme

The high-frequency internal oscillator operates at a nominal frequency of 120MHz. It is the primary clock source for the digital logic and peripherals. Select a 7.3728MHz internal oscillator to optimize active power consumption. A nanopower 8kHz ring oscillator is also available. Wakeup is possible from either the 7.3728MHz internal oscillator or the 120MHz internal oscillator.

ChipDNA Physically Unclonable Function (PUF)

Physically unclonable functions exploits the natural silicon manufacturing variations to generate unpredictable values that are statistically unique per chip. The MAX32520 uses PUF to generate unique keys while providing ultimate resistance against reverse-engineered based attacks.
The PUF instance present in the MAX32520 generates the flash encryption key. It can also provide a unique ECDSA private key for device strong authentication. The associated public key can be further exported and signed by a certification authority.

True Random Number Generator

Random numbers are a vital part of a secure application, providing random numbers that can be used for cryptographic seeds or strong encryption keys to ensure data privacy.

Software can use random numbers to trigger asynchronous events that result in nondeterministic behavior. This is helpful in thwarting replay attacks or key search approaches. An effective true random number generator (TRNG) must be continuously updated by a high-entropy source.

The provided TRNG is continuously driven by a physically-unpredictable entropy source. It generates a 128-bit true random number in 128 system clock cycles.

The TRNG can support the system-level validation of many security standards such as FIPS 140-2, SP800-90, PCI-PED, and Common Criteria. Contact Maxim for details of compliance with specific standards.

Serial Flash Emulation

One of the SPI ports provides the ability for a host microcontroller to use the device as an external serial flash for secure boot. The full capacity of flash memory is accessible and the amount of flash accessible can also be restricted. This feature provides a highly secure boot function for non-secure host microcontrollers. The device recognizes serial flash JEDEC commands.

Cryptographic Functions

AES Engine

The dedicated hardware-based AES engine supports the following algorithms:

- AES-128
- AES-192
- AES-256

ECDSA Engine

The ECDSA engine enables ECDSA signature and verification for following key lengths:

- 256 bits
- 384 bits
- 521 bits

Brainpool and NIST curves are supported.

SHA Engine

The SHA engine supports following SHA algorithms:

- SHA-1
- SHA-256
- SHA-384
- SHA-512

RSA

A crypto API enables RSA computation with key lengths up to 4096 bits.

UART

The universal asynchronous receiver-transmitter (UART) interface supports full-duplex asynchronous communication, including:

- 16-byte send/receive FIFO
- Full-duplex operation for asynchronous data transfers
- Interrupts available for frame error, parity error, Rx FIFO overrun, and FIFO full/partially full conditions
- Automatic parity and frame error detection
- Independent baud-rate generator
- Programmable 9th bit parity support
- Multidrop support
- Start/stop bit support
- Baud Rate Generation with ±2%
- Maximum baud rate 1843.2kB
- Two DMA channels can be connected (read and write FIFOs)
- Programmable word size (5 bits to 8 bits)

Note: No hardware flow control using RTS/CTS.

I^2C Interface

The I^2C interface is a bidirectional, two-wire serial bus that provides a medium-speed communications network. It can operate as a one-to-one, one-to-many or many-to-many communications medium. The I^2C master/slave interface to a wide variety of I^2C-compatible peripherals. This engine support both standard mode and fast mode I^2C standards. It provides the following features:

- Master or slave mode operation
- Supports standard (7-bit) addressing or 10-bit addressing

- Support for clock stretching to allow slower slave devices to operate on higher speed busses
- Multiple transfer rates
  - Standard mode: 100kbps
  - Fast mode: 400kbps
  - Fast mode plus: 1000kbps
- Internal filter to reject noise spikes
- Receiver FIFO depth of 16 bytes
- Transmitter FIFO depth of 16 bytes

SPI

The serial peripheral interface (SPI) is a synchronous interface allowing multiple SPI-compatible devices to be interconnected.

The provided SPI supports the following features:

- Full-duplex, synchronous communication of 8-/16-bit characters
- 4-wire interface plus
  - 1 additional slave select (SPI0)
  - 3 additional slave selects (SPI1)
- Master and slave mode of operation
- Master mode data transfer rate of up to one-fourth of the APB clock frequency
- Slave mode data transfer rate of up to one-eighth of the APB clock frequency
- Dedicated baud rate generator
- 8 x 16 transmit and receive FIFOs
- Transmit and receive DMA support

The MAX32520 has two SPI ports SPI0 and SPI1.

Debug and Development Interface (SWD/JTAG)

Development versions of the device are available with a serial wire debug or JTAG interface that is used only during application development and debugging. The interface is used for code loading, ICE debug activities and for control of boundary scan activities. Devices in mass production must have the debugging/development interface disabled.

The Ordering Information section contains unique part numbers for devices with the debugging/development interface enabled or disabled.

Interrupt Sources

The Arm nested vector interrupt controller (NVIC) provides a high-speed, deterministic interrupt response, interrupt masking, and multiple interrupt sources. Each peripheral is connected to the NVIC and can have multiple interrupt flags to indicate the specific source of the interrupt within the peripheral.

Standard DMA Controller

The standard DMA (direct memory access) controller provides a means to off-load the CPU for memory/peripheral data transfer leading to a more power-efficient system. It allows automatic one-way data transfer between two entities. These entities can be either memories or peripherals. The transfers are done without using CPU resources. The following transfer modes are supported:

- 4 channel
- Peripheral to data memory
- Data memory to peripheral
- Data memory to data memory

All DMA transactions consist of an AHB burst read into the DMA FIFO followed immediately by an AHB burst write from the FIFO.

Programmable Timers

Four 32-bit timers provide timing, capture/compare, or generation of pulse-width modulated (PWM) signals.

- 32-bit up/down autoreload
- Programmable 16-bit prescaler
- PWM output generation
- Capture, compare, and capture/compare capability
- GPIOs can be assigned as external timer inputs, clock gating or capture, limited to an input frequency of 1/4 of the peripheral clock frequency
- Timer output pin
- Timer interrupt

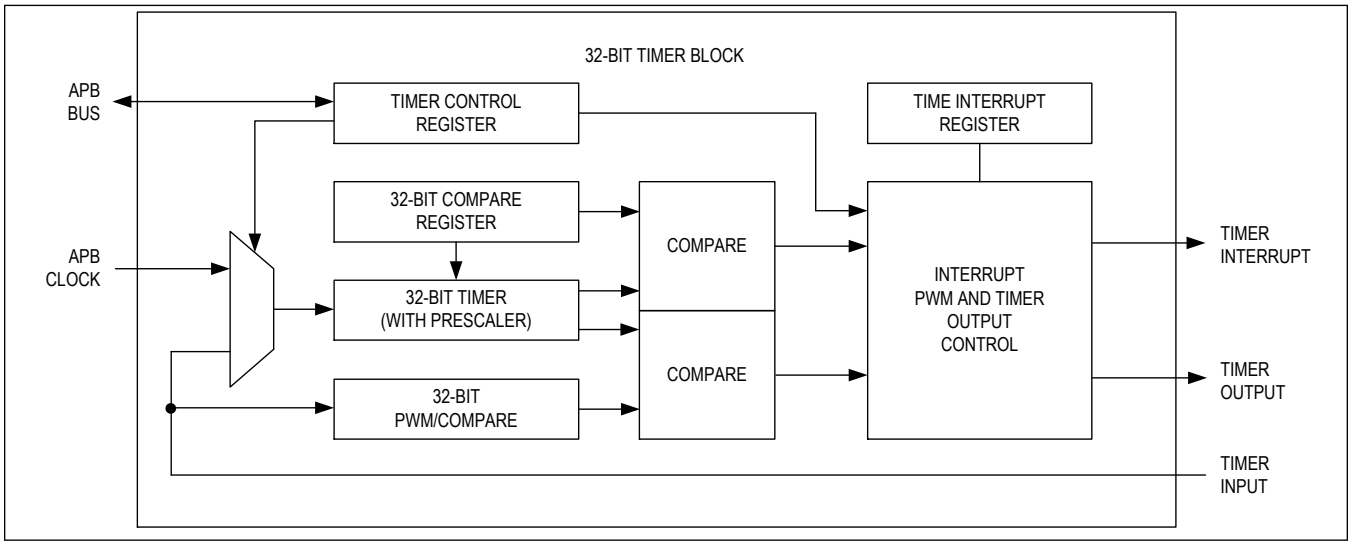


Figure 4. Timer Block Diagram, 32-Bit Mode

Watchdog Timer

A watchdog timer (WDT) is provided. The watchdog uses a 32-bit timer with prescaler to generate the watchdog reset. When enabled, the watchdog timer must be written prior to timeout. Failure to write the watchdog timer prior to the pre-programmed interval time results in a watchdog timeout. The WDT1 is set on reset if a watchdog expiration caused the system reset. The clock source for the watchdog timer is the system clock.

Power Management

Active Mode

In this mode, the CPU is executing application code and all digital and analog peripherals are available on-demand. Dynamic clocking disables peripherals not in use, providing the optimal mix of high-performance and low-power consumption.

Sleep Mode

This mode consumes less power, but wakes faster because the clocks can optionally be enabled.

The device status is as follows:

- The CPU is asleep
- Peripherals are on
- Standard DMA blocks are available for optional use.

DeepSleep Mode

This mode corresponds to the Arm Cortex-M4 DeepSleep mode. In this mode, CPU and critical peripheral configuration settings and all volatile memory is preserved.

The device status is as follows:

- The CPU is off.
- The GPIO pins retain their state.
- The transition from DeepSleep to Active mode is faster than the transition from Backup mode because system initialization is not required.
- The system oscillators are all disabled to provide additional power savings over Sleep mode.
  - 120MHz high-speed oscillator
  - 7.3728MHz oscillator

Backup Mode

This mode places the CPU in a static, low-power state that supports a fast wake-up to Active mode feature.

The device status is as follows:

- CPU is off.
- Only 72KB, 64KB, 32KB, or 8KB of the SRAM can be retained.

Wake-Up Sources

The sources of wake-up from the Sleep, DeepSleep, and Backup operating modes can be summarized in Table 1.

Table 1. Wake-Up Sources

OPERATING MODE	WAKE-UP SOURCE
Sleep	Interrupts (GPIO, all peripherals), RSTN assertion
DeepSleep	Interrupts (GPIO), RSTN assertion
Backup	Interrupts (GPIO), RSTN assertion

Security Monitor

Internal Sensor

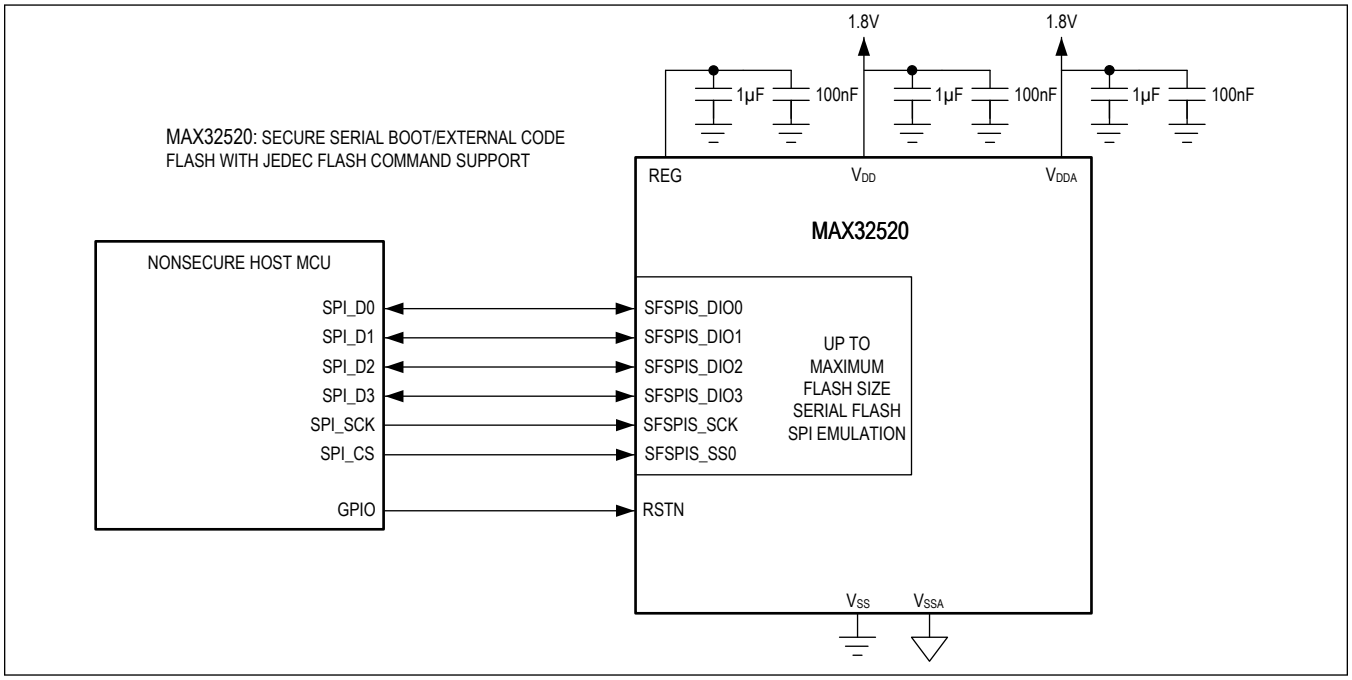
The behavior of the system is constantly monitored by a range of internal sensors. The internal sensors include environmental sensors such as die shield sensor, fault detection sensors and temperature sensor. Furthermore, there are core sensors monitoring internal core voltage on all rails.

External Tamper Sensors

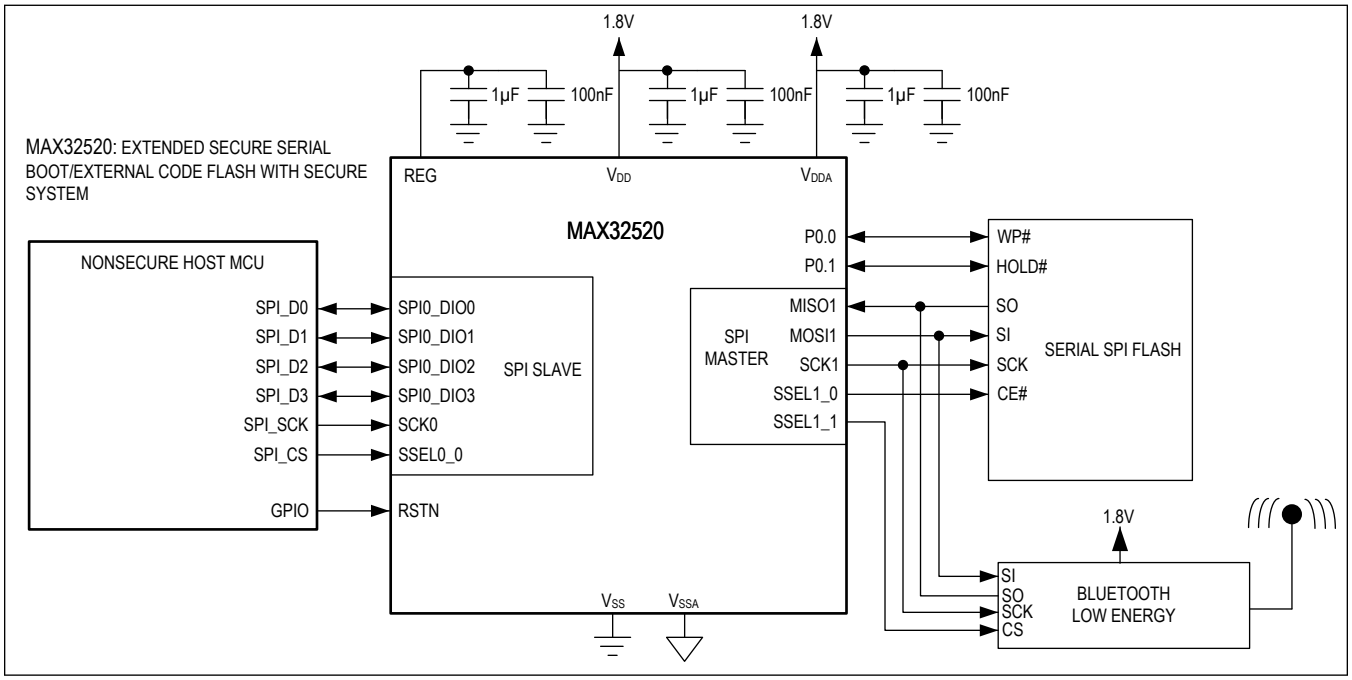
The device provides an external dynamic tamper sensor. The external tamper sensor uses two pins (EXT_SENSOR_IN, EXT_SENSOR_OUT) that provide a random, changing pattern generated by an internal, true random entropy source. The two pins can be connected to a mesh or user-defined, normally-closed tamper switch. External tamper detection triggers both predefined and user-customizable reactions. Tamper detection also toggles the TAMPER_OUT pin so that MAX32520 can signal tamper detection to external devices.

Typical Application Circuits

Secure Serial Boot/External Code Flash with JEDEC Flash Command Support



Extended Secure Serial Boot/External Code Flash with Secure System



Ordering Information

PART	DEBUG INTERFACE	PIN-PACKAGE
MAX32520-BNJ+	Yes	32 TQFN
MAX32520-BNS+	No	32 TQFN
MAX32520-BNS+T	No	32 TQFN
MAX32520/W+JU*	Yes	30 WLP
MAX32520/W+U*	No	30 WLP
MAX32520/W+T*	No	30 WLP

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

T = Tape and reel. Full reel.

**Future product—contact factory for availability.*

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	6/19	Initial release	—

For pricing, delivery, and ordering information, please visit Maxim Integrated's online storefront at https://www.maximintegrated.com/en/storefront/storefront.html.