Low-Power Arm Cortex-M4 Microcontroller with Contactless Radio for Secure Applications

General Description

The MAX32570 DeepCover® secure microcontroller provides an interoperable, secure, and cost-effective solution to build new generations of trusted devices. It can be used in single-chip applications such as PIN pads, mobile POS (MPOS), and secure card reader for PIN (SCRP), but also in dual-chip applications such as countertop and tablet POS. It includes all the essential functions to address those applications including a multi-protocol RF contactless controller and radio front-end, a dual smart card controller, a parallel camera interface, a magnetic stripe reader (MSR), a TFT controller, and a secure keypad controller.

The MAX32570 operates at 150MHz and is based on an Arm® Cortex®-M4 with FPU processor with 1MB flash, 760KB SRAM, 8KB OTP, 1KB of battery-backed AES self-encrypted nonvolatile SRAM (NVSRAM) and a 256-bit flip-flop-based battery-backed key storage. The flash memory is split into two banks of 512KB to provide flexibility when programming over the air. Error correction coding (ECC) (single-error correction double-error detection, or SEC-DED) for flash and SRAM provides extremely reliable code execution. The device embeds both secure public and private key cryptographic algorithms and a true random number generator (TRNG) compliant with SP-800-90A and SP-800-90B standards. It also features a number of security protections and detectors to enforce system integrity including a dynamic sensor controller, environmental sensors, and fault detectors.

The device features five flexible power modes. Multiple SPI, UART, and I2C serial interfaces, as well as a QSPI, 1-Wire® master, a USB 2.0 High-Speed device, and an optional 10/100 Ethernet MAC, allow for greater connectivity. Some device package variants offer flexible off-chip memory expansion that supports SD/SDHC, SDIO/eMMC cards, QSPI flash, and SRAM memories with eXecute In Place (XIP), encryption, and authentication. The device is available in a number of package variants, ranging from 121-pin BGA to 169-pin BGA, 0.65mm pitch packages.

Applications

- Secure Card Reader for PIN (SCRP)
- PCI Mobile Payment Terminals (MPOS)
- Countertop and Tablet POS
- Contact/Contactless PIN Pads
- ATM Keyboards

Benefits and Features

- High-Efficiency Microcontroller for Secure Battery-Powered Applications
  - Arm Cortex-M4 Processor with FPU up to 150MHz
  - 150MHz and 75MHz Internal Oscillators
  - Low-Power 7.37MHz System Clock Option
  - 1MB Flash, Organized into Dual Banks 2 x 512KB
  - 760KB (608KB ECC) SRAM
  - Optional Error Correction Code (ECC-SEC-DED) for Cache, SRAM, and Internal Flash
  - 1KB AES Encrypted NVSRAM, 8KB Internal OTP
- Scalable Cached External Memory Interfaces
  - QSPI Flash with AES-GCM and XiP
  - QSPI SRAM with AES-GCM and XiP
  - 150Mbps SDHC/eMMC/SDIO/microSD Interface
- Security Features Facilitates System-Level Protection
  - ISO 14443A/B, JIS X 6319-4, ISO 15693 Contactless Reader with Internal Transceiver
  - Secure Bootloader with Public Key Authentication
  - Hardware AES, DES, ECDSA, and SHA-2 Engines
  - 10-Line Secure Keypad Controller
  - TRNG (SP-800-90A and SP-800-90B)
  - Six External Dynamic Tamper Sensors
  - Die Shield with Dynamic Random Signal
  - 1x 256-Bit and 2x 128-Bit Flip-Flop-Based AES Key Storage
  - Temperature and Voltage Tamper Monitor
  - Fault Detectors
- Optimal Peripheral Mix Provides Platform Scalability
  - 16-Channel DMA
  - One QSPI/SPI Master
  - Up to Three SPI Master (37.5MHz)/Slave (75MHz)
  - Up to Six UARTs with Flow Control
  - Up to Two ISO 7816 UART/Smart Card Controller
  - Up to Three 1MHz I2C Master/Slave
  - Up to Three Channels 7.8ksps 10-Bit Sigma-Delta ADC
  - USB 2.0 High-Speed Device Interface with PHY
  - 10/100 Ethernet MAC with RMII/MII Support
  - 24-Bit TFT LCD Controller
  - 12-Bit Parallel Camera Interface
  - Triple-Track Magnetic Stripe Head Interface
  - Eight Pulse Train Generators
  - Six 32-Bit Timers, Two HTimers
  - 1-Wire Master, Two Watchdog Timers
  - Real-Time Clock (RTC)

Arm and Cortex are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
DeepCover and 1-Wire are registered trademarks of Maxim Integrated Products, Inc.

Visit Web Support to complete the nondisclosure agreement (NDA) required to receive additional product information.

Rev. 6

Information furnished by Analog Devices is believed to be accurate and reliable. However, no responsibility is assumed by Analog Devices for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implicationor otherwise under any patent or patent rights of Analog Devices. Trademarks andregistered trademarks are the property of their respective owners.