MAXQ1010

DeepCover Secure Microcontroller with RTC and USB for Secure Tokens

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 (MAXQ1010) is a small, low-cost, low-power secure microcontroller designed for security token applications and battery-powered applications where power and security are both critically important.

The microcontroller contains a 128KB programmable flash memory that can be used for both application code and data storage. Each 512B flash memory page supports 20,000 erase cycles and is programmable 16 bits at a time. This allows for unique schemes to extend the lifetime of the flash. For instance, dedicating four flash pages to store 32B of data that changes very often, the effective number of write cycles can approach 1.2 million (4 x 512 x 20,000/32). The device also contains 2KB SRAM. An additional 128B secure key storage SRAM is instantly erased when a self-destruct input is detected.

The microcontroller also contains a hardware DES engine and an AES accelerator, allowing applications to quickly respond to challenges and authenticate other devices using standards-based cryptography. A true-hardware random-number generator (RNG) is available for general application use, such as key generation, challenge generation, and random padding. Firmware and reference designs are available from Maxim Integrated for authentication applications.

Multiple communication interfaces are implemented: an integrated USB transceiver and serial interface engine make USB applications extremely low cost; also included are an ISO 7816 UART, SPI, I²C, and a standard USART (universal synchronous/asynchronous receiver-transmitter). A real-time clock (RTC) is also included for security applications requiring a time base.

For the ultimate in low-power battery-operated performance, an ultra-low-power stop mode (400nA typ) is included. In this mode, the minimum amount of circuitry is powered. Wake-up sources include external interrupts, the power-fail interrupt, a wake-up timer interrupt, and an RTC interrupt.

Applications

- One-Time Password Generator
- USB Card Readers

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

Features

- High-Performance, Low-Power, 16-Bit RISC Core
- DC to 12MHz Operation Across Entire Operating Range
- 6MHz Internal Oscillator
- 12MHz External Crystal (Required for USB Operation)
- 1.7V to 3.6V Operating Voltage Range
- Three Independent Data Pointers Accelerate Data Movement with Automatic Increment/Decrement
- Dedicated Pointer for Direct Read from Code Space
- 16-Bit Instruction Word, 16-Bit Data Bus
- 1-Wire® Interface for Debugger and Flash Programming
- Security Features
  - DES and AES Hardware Accelerators
  - Hardware True RNG
  - Self-Destruct Input Pin
  - 128B, Fast Wipe, Secure Secret Key SRAM
  - RTC with Integrated Oscillator
- Memory
  - 128KB Flash
    - 512-Byte Memory Page Sectors
    - 20,000 Erase/Write Cycles per Sector
  - 2KB Data SRAM
  - Dedicated Utility ROM with User-Callable Routines
- I/O and Peripherals
  - USB 2.0 SIE and Transceiver
  - SPI, USART, and I²C Communication Ports
  - ISO 7816 UART
  - Two 16-Bit Timers
  - 31 General-Purpose I/O Pins
  - Up to 15 External Interrupts Available
- Low Power Consumption
  - Single 1.7V to 3.6V Supply
  - < 1µA Current in Lowest Power Stop Mode
  - Divided System Clock Modes Available
- Additional Peripherals
  - Power-Fail Warning
  - Power-On Reset (POR)
  - Programmable Watchdog Timer

For related parts and recommended products to use with this part, refer to www.maximintegrated.com/MAXQ1010.related.

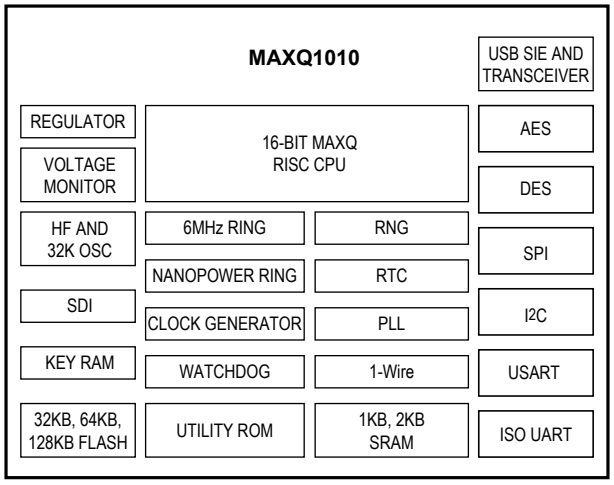
***Ordering Information* appears at end of data sheet.**

ABRIDGED DATA SHEET

19-5259; Rev 1; 7/13

maxim integrated™

Block Diagram



ABRIDGED DATA SHEET

Note to readers: This document is an abridged version of the full data sheet. To request the full data sheet, go to www.maximintegrated.com/MAXQ1010 and click on **Request Full Data Sheet**.

For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

Maxim Integrated cannot assume responsibility for use of any circuitry other than circuitry entirely embodied in a Maxim Integrated product. No circuit patent licenses are implied. Maxim Integrated reserves the right to change the circuitry and specifications without notice at any time. The parametric values (min and max limits) shown in the Electrical Characteristics table are guaranteed. Other parametric values quoted in this data sheet are provided for guidance.

