EVALUATION KIT AVAILABLE

MAXQ1850

DeepCover Secure Microcontroller with Rapid Zeroization Technology and Cryptography

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 (MAXQ1850) is a low-power, 32-bit RISC device designed for electronic commerce, banking, and data security systems. It combines high-performance, single-cycle processing, sophisticated tamper-detection technology, and advanced cryptographic hardware to provide industry-leading data security and secret key protection.

Physical security mechanisms include environmental sensors that detect out of range voltage or temperature conditions, responding with rapid zeroization of critical data. Four self-destruct inputs are provided for additional tamper response. An internal shield over the silicon provides protection from microprobe attacks. A high-speed internal ring oscillator is provided to thwart attacks that rely on controlling the clock rate of the chip. To protect data, the MAXQ1850 integrates several high-speed, analysis-resistant encryption engines. Algorithms supported in hardware include AES (128-, 192-, and 256-bit), DES, triple DES (2-key and 3-key), ECDSA (160-, 192-, and 256-bit keys), DSA, RSA (up to 2048 bits), SHA-1, SHA-224, and SHA-256. The advanced security features of the MAXQ1850 are designed to meet the stringent requirements of regulations such as ITSEC E3 High, FIPS 140-2 Level 3, and the Common Criteria certifications.

The MAXQ1850 includes 256KB of flash memory and 8KB of secure, battery-backed data SRAM. Several communication protocols are supported with hardware engines, including ISO 7816 for smart card applications, USB (slave interface with four end-point buffers), an RS-232 universal synchronous/asynchronous receiver-transmitter (USART), an SPI interface (master or slave mode support), and up to 16 general-purpose I/O pins. Other peripherals supported on the MAXQ1850 include a true hardware random-number generator (RNG), a real-time clock (RTC), a programmable watchdog timer, and flexible 16-bit timers that support capture, compare, and pulse-width modulation (PWM) operations.

DeepCover is a trademark of Maxim Integrated Products, Inc.

EMV is a registered trademark of EMVCo LLC.

Features

- **High-Performance, Low-Power, 32-Bit MAXQ30 RISC Core**
- **Single 3.3V Supply Enables Low Power/Flexible Interfacing**
- **DC to 16MHz Code Execution Across Entire Operating Range**
- **65MHz Cryptography Engine Execution to Reduce Processing Time**
- **On-Chip 2x/4x Clock Multiplier**
- **33 Instructions**
- **16-Bit Instruction Word, 32-Bit Internal Data Bus**
- **16 x 32-Bit Accumulators**
- **Up to 16 General-Purpose I/O Pins**
- **5V Tolerant I/O**
- **Virtually Unlimited Software Stack**
- **Optimized for C-Compiler (High-Speed/Density Code)**
- **Memory Features**
- **Security Features**
- **Additional Peripherals**
- **Low-Power Consumption**

See the Detailed Features *section for complete list of features.*

Applications

Electronic Commerce	Pay-per-Play
EMV® Banking	Certificate Authentication
Secure Access Control	Electronic Signature Generation
Secure Data Storage	

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAXQ1850-BNS+	-40°C to +85°C	40 TQFN-EP*
MAXQ1850-LNS+	-40°C to +85°C	49 CSBGA
MAXQ1850-DNS+	-40°C to +85°C	Bare die

+Denotes a lead(Pb)-free/RoHS-compliant package.
**EP = Exposed pad.*

Selector Guide appears at end of data sheet.

Note: *Some revisions of this device may incorporate deviations from published specifications known as errata. Multiple revisions of any device may be simultaneously available through various sales channels. For information about device errata, go to: www.maximintegrated.com/errata.*

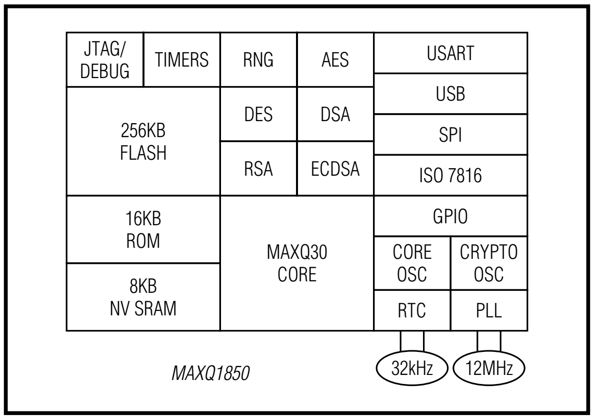
For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

ABRIDGED DATA SHEET

MAXQ1850

DeepCover Secure Microcontroller with Rapid Zeroization Technology and Cryptography

Block Diagram



NOTE: THE BLOCK DIAGRAM SHOWS A TYPICAL SYSTEM CLOCK USED TO SUPPORT USB OPERATION AT 12MHz. MULTIPLE EXTERNAL CRYSTAL/CLOCK OPTIONS ARE AVAILABLE.

Detailed Features

- **High-Performance, Low-Power, 32-Bit MAXQ30 RISC Core**
- **Single 3.3V Supply Enables Low Power/Flexible Interfacing**
- **DC to 16MHz Code Execution Across Entire Operating Range**
- **65MHz Cryptography Engine Execution to Reduce Processing Time**
- **On-Chip 2x/4x Clock Multiplier**
- **33 Instructions**
- **Three Independent Data Pointers Accelerate Data Movement with Automatic Increment/Decrement**
- **16-Bit Instruction Word, 32-Bit Internal Data Bus**
- **16 x 32-Bit Accumulators**
- **Up to 16 General-Purpose I/O Pins**
- **5V Tolerant I/O**
- **Virtually Unlimited Software Stack**
- **Optimized for C-Compiler (High-Speed/Density Code)**
- **Memory Features**
  - 256KB Flash, Composed of 2048 Byte Sectors (1K Erase/Write Cycles per Sector)
  - 8KB Battery-Backed Data SRAM
  - Dedicated Cryptographic Memory Space
- **Security Features**
  - Unique ID
  - Tamper Detection with Rapid Key/Data Destruction
  - Four Self-Destruct Inputs
  - Hardware AES and DES Engines
  - Public Key Cryptographic Accelerator for DSA, ECDSA, and RSA
  - Supports SHA-1, SHA-224, and SHA-256
  - Real Hardware RNG and PRNG
  - Hardware CRC-32/16
  - Unalterable, Battery-Backed Real-Time Clock
- **Additional Peripherals**
  - Power-Fail Warning
  - Power-On Reset/Brownout Reset
  - JTAG I/F for System Programming and Accessing On-Chip Debugger
  - USB I/F with Four End-Point Buffers
  - ISO 7816 Smart Card UART with FIFO
  - Four 16-Bit Timer/Counters, Two with PWM Function
  - SPI and USART Communication Ports
  - Programmable Watchdog Timer
- **Low-Power Consumption**
  - 150nA Typical Current Draw in Battery-Backed Mode, Preserving 8KB NV SRAM and with Security Sensors Active (460nA with RTC Active)

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/MAXQ1850 and click on **Request Full Data Sheet**.