ABRIDGED DATA SHEET

MAXQ1851

DeepCover Secure Microcontroller with Fast Wipe 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 (MAXQ1851) 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 MAXQ1851 integrates several high-speed 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 device's advanced security features 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 MAXQ1851 includes 256KB of flash memory, 8KB of SRAM, 4KB of AES encryptable battery-backed SRAM, and 256-bit secure, battery-backed, flip-flop-based key storage. 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 MAXQ1851 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.

Applications

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

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

For related parts and recommended products to use with this part, refer to www.maximintegrated.com/MAXQ1851.related.

DeepCover is a registered 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
- On-Chip 2x/4x Clock Multiplier
- 33 Instructions
- 16-Bit Instruction Word, 32-Bit Internal Data Bus
- 16 x 32-Bit Accumulators
- Virtually Unlimited Software Stack
- Optimized for C-Compiler (High-Speed/Density Code)
- Security Features
  - 65MHz Cryptography Engine Execution to Reduce Processing Time
  - Unique ID
  - Tamper Detection with Fast Wipe Key/Data Destruction
  - 4 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
  - True Hardware RNG and PRNG
  - Unalterable, Battery-Backed RTC
  - Hardware CRC-32/16
- Memory
  - 256KB Flash, Composed of 2048-Byte Pages (20K Erase/Write Cycles per Sector)
  - 8KB SRAM, 4KB Battery-Backed SRAM
  - 256-Bit, Battery-Backed, Flip-Flop-Based Secure Key Storage
  - Dedicated Cryptographic Memory Space
- I/O and Peripherals
  - Up to 16 General-Purpose I/O Pins
  - 5V Tolerant I/O
  - 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
  - 4 16-Bit Timer/Counters, Two with PWM Function
  - SPI and USART Communication Ports
  - Programmable Watchdog Timer
- Low-Power Consumption
  - 550nA typ Current Draw in Battery-Backed Mode, Preserving 4KB AES Encryptable NV SRAM and 256-Bit Flip-Flop-Based Secure Master Key Storage, with Security Sensors Active (1.5µA with RTC and Active Die Shield Enabled)

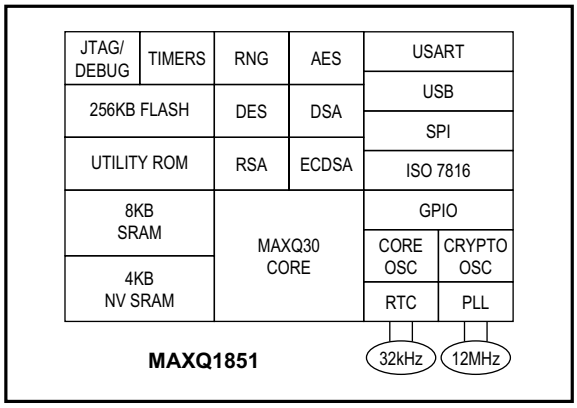
19-6618; Rev 0; 5/13

maxim integrated™

MAXQ1851

DeepCover Secure Microcontroller with Fast Wipe 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 Description

The MAXQ1851 is designed for electronic commerce, banking, and data security systems that require secure access control, secure data storage, digital signature, or certificate authentication. For example, it can be used for PIN pads and to act as a coprocessor for higher end POS terminals. The controller combines low power operation with high-performance cryptographic accelerators, advanced security features, and advanced semiconductor process technologies to meet the most stringent needs of security applications. Sensitive data such as keys are shielded within and never need to leave the MAXQ1851, thwarting PCB level attacks. On-chip tamper sensors and an internal active die shield deter physical attacks against the device. Custom-designed cryptographic hardware and unique countermeasures protect against logical and statistical attacks, such as differential or simple power analysis. The MAXQ1851 provides self-destruct inputs (SDI1−SDI4) as well as a multitude of environmental monitors including temperature, battery voltage, and V_{DD} voltage.

The MAXQ1851 offers a rich set of peripherals including serial I/O, SPI, USB, and ISO 7816 smart card interfaces for efficient communication. Each MAXQ1851 has a universally unique identification number for device management and to prevent cloning.

The MAXQ1851 contains the hardware-accelerated cryptography units required for system certification under ITSEC E3 High, FIPS 140-2 Level 3, Common Criteria, and the USPS PCIBI-C standard. The MAXQ1851 is designed to meet the security requirements of the Visa PCI (Payment Card Industry) specification as part of an overall system solution.

The cryptographic accelerator supports both symmetric cryptography (AES, DES, 3DES, both two-key and three-key) and asymmetric cryptography (RSA, DSA, ECC). The MAXQ1851 can internally generate, store, and check digital signatures (DSA, ECDSA, RSA), secure hash algorithms (SHA), and cryptographic keys; a secure, FIPS 186-2-compliant hardware RNG and an RTC are built into the device.

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAXQ1851-BNS+	-40°C to +85°C	40 TQFN-EP*

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

**EP = Exposed pad.*

Note to readers: This document is an abridged version of the full data sheet. Additional device information is available only in the full version of the data sheet. To request the full data sheet, go to **www.maximintegrated.com/MAXQ1851** and click on **Request Full Data Sheet**.