MAXQ1741

DeepCover Secure Microcontroller for Magnetic Card Reading

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 (MAXQ1741) is a low-power microcontroller that integrates a triple-track magnetic stripe reader interface, an I²C interface, two SPI interfaces, and one universal synchronous/asynchronous receiver-transmitter (USART) interface. Security features include an AES encryption engine, a true hardware random-number generator, voltage-attack sensors, and a self-destruct input pin. A single-cycle 16-bit RISC MAXQ® CPU powers the device. It provides a high level of security for the magnetic stripe reader by placing an ultra-secure microcontroller with high-speed hardware encryption inside the magnetic card reader head.

The device provides 16KB of flash memory and 1152 bytes of fast-wipe nonvolatile SRAM (NV SRAM) that clear its contents when a tamper is detected. The highest 128 bytes of the NV SRAM can be used as data RAM or working RAM for the AES. The fast-wipe feature ensures that any data in the 1152 bytes of memory is destroyed before any application software can access it. Factory programming of a unique 64-bit serial number, and/or customer secret key(s), is available upon request. The microcontroller runs within a wide 1.7V to 3.6V operating range. User-application firmware interfaces with the triple-track magnetic stripe interface. Reference software supports the reading of cards adhering to ISO 7811, ISO 7812, and ISO 7813. Source code to the reference software is available so applications can make adjustments for custom card formats.

An ultra-low-power stop mode provides the ultimate in low-power performance. In this mode, only a minimum amount of circuitry is powered to support detection of self-destruct events. When the main power supply is present and the microcontroller is in stop mode, the device has the option of exiting stop mode when stimulated by general-purpose port pins or the serial interfaces.

Applications

ATM/POS Terminals

Physical Security/Building Access

Features

- **Core Functionality**
  - **High-Performance, Low-Power, 16-Bit MAXQ20C RISC Core**
  - **6MHz Internal Oscillator (±10%)**
  - **Up to 12MHz External Crystal Supported**
  - **1.7V to 3.6V Operating Voltage**
  - **1-Wire® Interface for Debugger and Flash Programming**
  - **Optimized for C-Compiler**
- **Security**
  - **AES Hardware Accelerators**
  - **Hardware True Random-Number Generator**
  - **Self-Destruct Input for Tamper Detection**
  - **Permanent Loader Lockout Option**
  - **Code Scrambling**
- **Memory**
  - **16KB Flash Memory**
    - **1024 Bytes Memory Page Sectors**
    - **1000 Erase/Write Cycles per Sector**
  - **1152 Bytes Fast-Wipe NV SRAM, 128 Bytes Usable by Cryptographic Engine**
  - **6KB Utility ROM with User-Callable Routines**
- **I/O and Peripherals**
  - **Triple-Track Magnetic Stripe Head Interface**
  - **Two SPI Communication Ports**
  - **USART Communication Port**
  - **Two 16-Bit Timers**
  - **I²C Communication Port**
  - **Up to 16 General-Purpose I/O Pins**
  - **Up to 8 External Interrupt Pins**
- **Low Power Consumption**
  - **3µA Current in Lowest Power Stop Mode**
  - **3.75mA (typ) at 6MHz, 0.8mA (typ) at 1MHz**
  - **Divided System Clock Modes Available**
- **Additional Peripherals**
  - **On-Chip Power-On/Power-Fail Reset**
  - **Supply Overvoltage Detection**
  - **Programmable Watchdog Timer**
  - **Wake-Up Timer**

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

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

For related parts and recommended products to use with this part, refer to: www.maximintegrated.com/MAXQ1741.related

***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.*

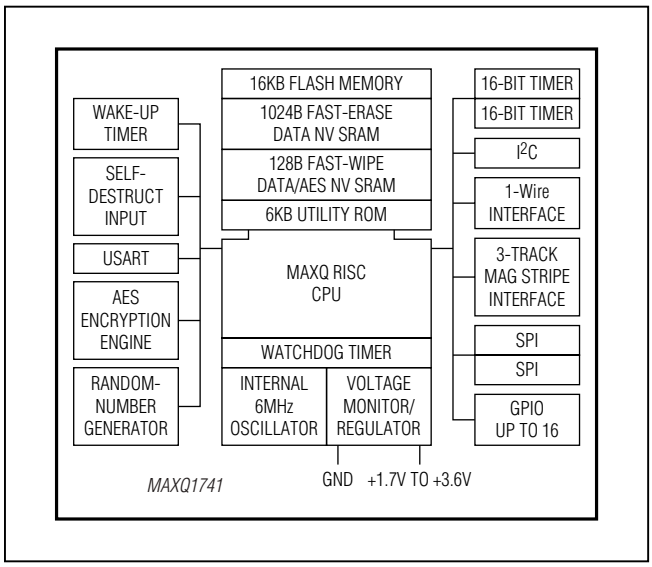
For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

19-6564; Rev 3; 7/14

MAXQ1741

DeepCover Secure Microcontroller for Magnetic Card Reading

Block Diagram



Detailed Description

The MAXQ1741 is a MAXQ20C-based microcontroller intended for integration into magnetic card readers. It can be interfaced directly to a 3-track magnetic card reader head, allowing security features to be added to a POS or ATM card reader right at the machine/card interface. Encryption is provided by a hardware AES engine. Security features include a self-destruct input for tamper detection, code scrambling, and fast-wiping of the NV SRAM in the event of a tamper detection and supply-rail monitoring for overvoltage conditions. A 16KB flash memory provides nonvolatile storage for user programs and other static, nonvolatile data.

The device provides 1152 bytes of fast-wipe NV SRAM that clears its contents when a tamper is detected. The highest 128 bytes of the NV SRAM can be used as data RAM or working RAM for the AES. The fast-wipe feature ensures that any data in the 1152 bytes of memory is destroyed before any application software can access it. Communication peripherals include a hardware I²C, a hardware USART, and two hardware SPIs. A 1-Wire port is available for system programming and application debugging.

Microprocessor

The MAXQ20C core supports the Harvard memory architecture with separate 16-bit program and data address buses. A fixed 16-bit instruction word is standard, but data can be arranged in 8 or 16 bits. The MAXQ core is implemented as a pipelined processor with performance approaching 1MIPS per MHz. The 16-bit data path is implemented around register modules, and each register module contributes specific functions to the core. The accumulator module consists of sixteen 16-bit registers and is tightly coupled with the arithmetic logic unit (ALU). Program flow is supported by a configurable soft stack.

Execution of instructions is triggered by data transfer between functional register modules, or between a functional register module and memory. Since data movement involves only source and destination modules, circuit switching activities are limited to active modules only. For power-conscious applications, this approach localizes power dissipation and minimizes switching noise. The modular architecture also provides a maximum of flexibility and reusability that are important for a microprocessor used in embedded applications.

The MAXQ instruction set is highly orthogonal. All arithmetic and logical operations can use any register in conjunction with the accumulator. Data movement is supported from any register to any other register. Memory is accessed through specific data pointer registers with auto increment/decrement support.

Memory

The microcontroller incorporates several memory types:

- 16KB flash memory
- 1152 bytes fast-wipe NV SRAM, including 128 bytes intended for use by the AES engine
- 6KB utility ROM
- RAM-based software stack

The NV SRAM is cleared by a DRS event. The 128-byte memory can be used as general-purpose memory if the AES function is not in use. Starting the AES engine invalidates data stored in this memory.

MAXQ1741

DeepCover Secure Microcontroller for Magnetic Card Reading

Additional Documentation

Designers must have the following documents to fully use all the features of this device. This data sheet contains pin descriptions, feature overviews, and electrical specifications. Errata sheets contain deviations from published specifications. The user's guides offer detailed information about device features and operation.

- This MAXQ1741 data sheet, which contains electrical/timing specifications and pin descriptions.
- The revision-specific MAXQ1741 errata sheet.
- The *MAXQ1740/MAXQ1741 User's Guide*, which contains detailed information on core features and operation, including programming.

Development and Technical Support

A variety of highly versatile, affordably-priced development tools for this microcontroller are available from Maxim and third-party suppliers, including:

- Compilers
- In-circuit emulators
- Integrated development environments (IDEs)

A partial list of development tool vendors can be found at **www.maximintegrated.com/MAXQ_tools**.

For technical support, go to **https://support.maximintegrated.com/micro**.

Ordering Information

PART	TEMP RANGE	OPERATING VOLTAGE (V)	FLASH MEMORY (KB)	DATA MEMORY (KB)	PIN-PACKAGE
MAXQ1741-FBX+	-40°C to +85°C	1.70 to 3.6	16	1	28 TQFN-EP*
MAXQ1741-DNS+	-40°C to +85°C	1.70 to 3.6	16	1	Bare die

Note: *Refer to the MAXQ174X User's Guide for more details.*
+Denotes a lead(Pb)-free/RoHS-compliant package.
**EP = Exposed pad.*

Package Information

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 TYPE	PACKAGE CODE	OUTLINE NO.	LAND PATTERN NO.
28 TQFN-EP	T2844+1	21-0139	90-0035

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/MAXQ1741** and click on **Request Full Data Sheet**.