MAXIM
INNOVATION DELIVERED®

19-5822; Rev 2; 11/11

EVALUATION KIT AVAILABLE

MAXQ1050

Secure USB Microcontroller with Asymmetric Cryptography

General Description

The MAXQ1050 is a low-power secure microcontroller designed for USB secure token and smart card reader applications that require certificate-based or other public key cryptographic schemes. The device also incorporates a sophisticated security mechanism to protect secret key data; two self-destruct inputs and environmental monitors (temperature and voltage sensors) erase secret key data when an attack condition is detected. The device has an integrated full-speed USB device interface (including transceiver), hardware SPI controller, and an ISO 7816 UART (universal asynchronous receiver-transmitter) for smart card communication. The device supports high-speed encryption with hardware accelerators for AES, RSA, DSA, ECDSA, SHA-1, SHA-224, SHA-256, DES, and 3DES. A true hardware random-number generator is included for key generation and challenge generation.

The device uses the 32-bit, pipelined, highly efficient MAXQ30 microcontroller core. It integrates 128KB flash memory, 12KB of volatile SRAM, 4KB of battery-backed erasable NV SRAM, and 256B of battery-backed, secure zeroization NV SRAM. An additional 1.5KB of volatile cryptographic memory can also be used as general-purpose data memory. The 256B of battery-backed NV SRAM can be used for key storage and other critical data. The 256B memory can be erased in less than 1µs using a single pulse ("rapid zeroization"), even in battery-backed mode.

The device is powered either from the USB bus or by a separate 3.3V voltage supply. A battery connection is provided for applications that want to maintain secret key data for years without draining the battery from application use. In battery-backed mode, the NV SRAM and security sensors consume less than 240nA (typ). Battery backup is optional; applications can choose to store critical data in the flash memory when the cost of the battery outweighs the benefits of constant monitoring for tamper conditions.

Applications

- Security and Banking Tokens
- Certificate Management
- Electronic Signature Generation
- Smart Grid Security
- Prepaid Utility
- e-Commerce
- Secure Access Control
- Pay-per-Play

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

Features

- **High-Performance, Low-Power, 32-Bit MAXQ30 RISC Core**
- **Operates from USB Power or Single 3.3V Supply**
- **Runs from 20MHz (typ) Internal Oscillator**
- **Supports External 12/24MHz Crystal Oscillator for Microcontroller and USB Operation**
- **On-Chip 2x/4x Clock Multiplier**
- **16-Bit Instruction Word, 32-Bit Internal Data Bus**
- **16 x 32-Bit Accumulators**
- **16 x 32-Bit General-Purpose Working Registers**
- **Up to 20 General-Purpose I/O Pins**
- **5V Tolerant I/O**
- **Virtually Unlimited Software Stack**
- **Optimized for C-Compiler (High-Speed/Density Code)**
- **Memory**
  - **128KB Flash Memory, 512 x 32 Page Size**
  - **Flash Memory Supports 20k Erase/Write Cycles per Sector**
  - **256B of Secure NV SRAM**
  - **4KB Battery-Backed NV SRAM**
  - **12KB SRAM**
  - **Secure JTAG/TAP for In-System Programming and On-Chip Debugger Access**
- **Security**
  - **Unique 64-Bit Serial Number**
  - **Tamper Detection with Rapid Key/Data Destruction**
  - **Secret Key Destruction on Tamper Events**
  - **Permanent Loader Lockout Option**
  - **Proprietary Code Scrambling Technique Using Random Keys**
  - **Hardware Accelerators for AES, RSA, DSA, ECDSA, DES, 3DES, SHA-1, SHA-224, SHA-256**
  - **True Hardware Random-Number Generator**
  - **Temperature and Voltage Sensors to Detect Attacks**
  - **Two Self-Destruct Input Pins**
- **Additional Peripherals**
  - **Power-Fail Warning**
  - **Power-On-Reset/Brownout Reset**
  - **Full-Speed USB Device with Six Endpoint Buffers and Integrated Transceiver**
  - **ISO 7816 Smart Card UART with FIFO**
  - **16-Bit Programmable Timers/Counters with Prescaler, Capture/Compare, and PWM**
  - **SPI Master/Slave Hardware**
  - **Programmable Watchdog Timer**
  - **Up to 20 General-Purpose I/O Pins with Eight External Interrupts**

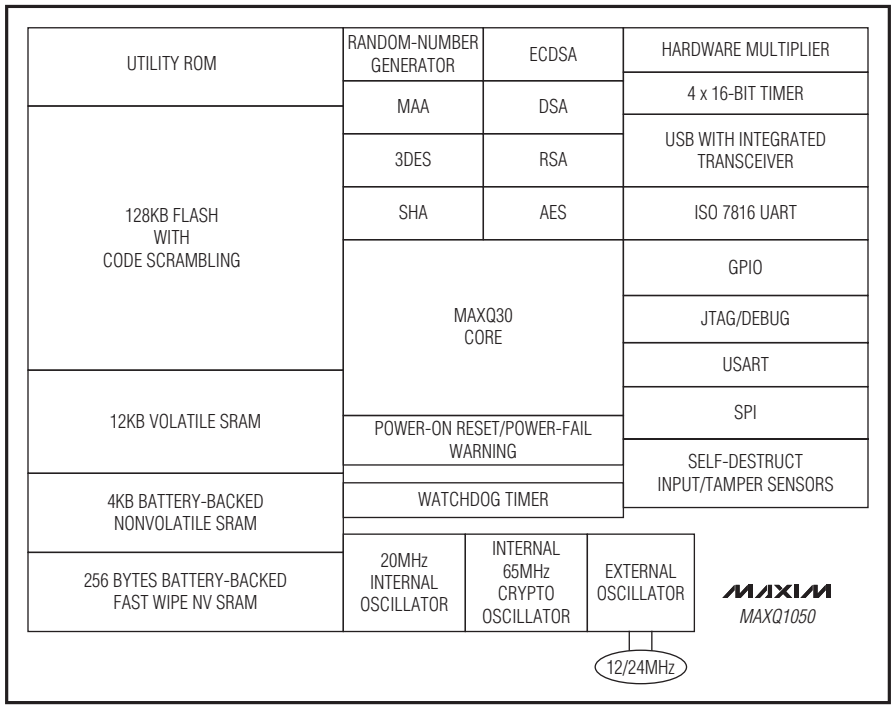
For related parts and recommended products to use with this part, refer to: ***www.maxim-ic.com/MAXQ1050.related***

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.maxim-ic.com/errata****.*

MAXQ1050

Secure USB Microcontroller with Asymmetric Cryptography

Block Diagram



MAXQ1050

Secure USB Microcontroller with Asymmetric Cryptography

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. User guides offer detailed descriptions of device features and peripherals from a programming perspective. The following documents can be obtained by contacting a technical support specialist.

- This MAXQ1050 data sheet, which contains electrical/timing specifications, package information, and pin descriptions.
- The MAXQ1050 revision-specific errata sheet.
- The *MAXQ1050 User's Guide*, which contains detailed information and programming guidelines for core features and peripherals.

Development and Technical Support

Maxim and third-party suppliers provide a variety of highly versatile, affordably priced development tools for this microcontroller, including the following:

- Compilers
- In-circuit emulators
- Integrated Development Environments (IDEs)
- JTAG-to-serial converters for programming and debugging

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

For technical support, go to **https://support.maxim-ic.com/micro**.

Ordering Information

PART	TEMP RANGE	FLASH PROGRAM MEMORY (KB)	DATA MEMORY	PIN-PACKAGE
MAXQ1050-BNS+	-40°C to +85°C	128	12KB SRAM 4KB NV SRAM 256B fast wipe NV SRAM	40 TQFN-EP*
MAXQ1050-DNS+	-40°C to +85°C	128	12KB SRAM 4KB NV SRAM 256B fast wipe NV SRAM	Bare die

+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.maxim-ic.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.
40 TQFN-EP	T4055+1	21-0140	90-0016

Note to readers: This document is an abridged version of the full data sheet. To request the full data sheet, go to **www.maxim-ic.com/MAXQ1050** and click on **Request Full Data Sheet**.