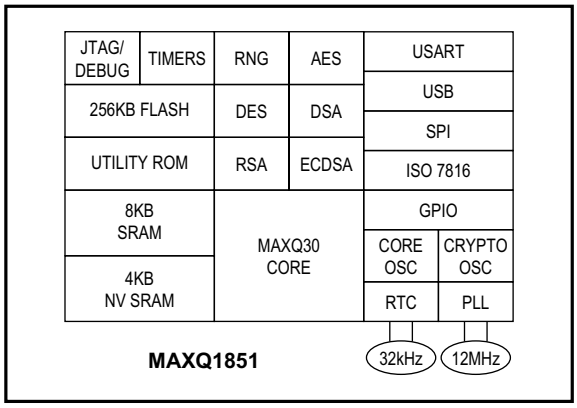
MAXQ1851

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**.