ABRIDGED DATA SHEET

*Click **here** for production status of specific part numbers.*

MAX32591

DeepCover Secure Microcontroller with ARM926EJ-S Processor Core

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 (MAX32591) provides an interoperable, secure, and cost-effective solution to build new generations of trusted devices such as multimedia-enabled portable EFT-POS terminals. The MAX32591 integrates a memory management unit (MMU), 32KB of instruction cache, 16KB of data cache, 4KB instruction TCM, 4KB data TCM, 384KB of system RAM, 2KB of one-time-programmable (OTP) memory, 128KB of boot ROM, and 24KB of battery-backed SRAM. The MAX32591 maximizes on-chip bandwidth when dealing with high-speed communication such as 100Mbps Ethernet, large color LCD displays, and gigabit-sized mass storage devices.

In addition to hardware crypto functions, the MAX32591 provides a true random number generator, battery-backed RTC, nonvolatile SRAM and real-time environmental and tamper detection circuitry to facilitate system-level security for the application.

The secure microcontroller includes multiple communication interfaces. One USB host controller and one USB device controller with their respective USB transceiver, two smart card controllers, five SPI ports, three UARTs, an Ethernet 10/100 MAC with FIFO, and an I^2C bus are also provided. The three on-chip timers also support PWM output generation for direct control of external devices. An integrated secure keypad provides an integrated solution for mobile POS terminals. Additionally, a 2-channel, 10-bit ADC is provided for printer support and general use.

Applications

- Electronic Commerce
- PCI Terminals
- PIN Pads
- ATM Keyboards
- EMV Card Readers
- Secure Access Control
- Secure Data Storage
- Pay-Per-Play
- Certificate
- Authentication
- Electronic Gaming

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

ARM926EJ-S is a trademark of ARM Limited.
DeepCover is a registered trademark of Maxim Integrated Products, Inc.

***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.*

Features and Benefits

- High Performance CPU platform Enables Feature Rich OS
  - ARM926EJ-S™ Processor Core with 16KB Data Cache and 32KB Instruction Cache
  - 4KB Instruction TCM, 4KB Data TCM
  - Up to 400MHz Core Operating Frequency
  - Up to 200MHz Multilayer AHB Bus Matrix
  - Up to 100MHz APB Bus Matrix
  - 384KB System SRAM
  - Flexible Clock Prescalers
  - Configurable Low-Power Modes
- Security Features Facilitates System-Level Protection
  - Secure Bootloader with Public Key Authentication
  - 256-Bit Flip-Flop-Based Nonvolatile AES Key Storage
  - 24KB AES User-Encryptable NV SRAM
  - 2KB User-Programmable OTP
  - AES, DES, and SHA Hardware Accelerators
  - Modulo Arithmetic Hardware Accelerator (MAA) Supporting RSA, DSA, and ECDSA
  - Secure Keypad Controller
  - Hardware True Random Number Generator
  - Die Shield with Dynamic Fault Detection
  - Six External Tamper Sensors with Independent Random Dynamic Patterns
  - Temperature and Voltage Tamper Monitor
  - Real-Time External Memory Encryption and Integrity Check
- 104-Bit Unique Serial Number (USN)
- Optimal Peripheral Mix Provides Platform Scalability
  - External Memory Controller (LPDDR400, SDRAM, SRAM, NOR Flash, NAND Flash)
  - NAND Flash Controller with Hardware ECC
  - USB 2.0 Host/Device with Internal Transceivers
  - Three UART Ports/One I^2C Port
  - Five SPI Ports with I^2S Functionality
  - Two ISO 7816 Smart Card Interfaces
  - 10/100Mbps Ethernet MAC Controller
  - Three Timers with PWM Capability
  - Up to 126 General-Purpose I/O Pins
  - 2-Channel, 10-Bit ADC
  - LCD Controller Supporting STN and TFT Displays
  - Monochrome LCD Controller
  - 16-Channel DMA Controller
  - Real-Time Clock
  - Advanced Interrupt Controller

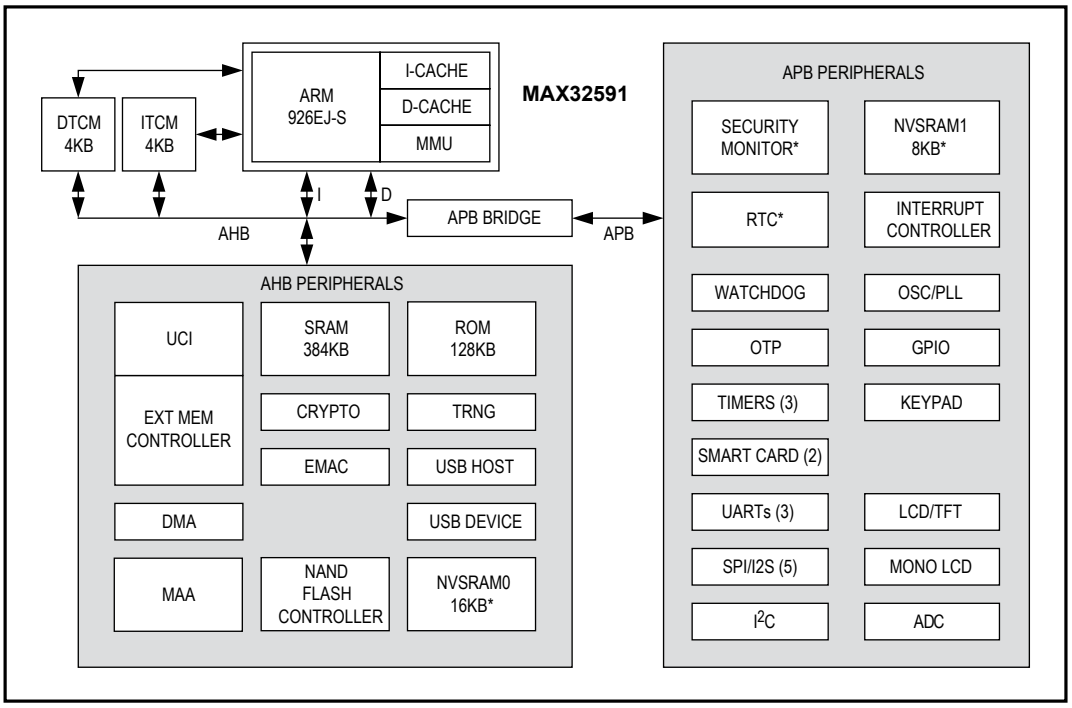
19-100430; Rev 1; 11/20

maxim integrated™

MAX32591

DeepCover Secure Microcontroller with ARM926EJ-S Processor Core

Functional Diagram



*BATTERY-BACKED CIRCUITRY

ABRIDGED DATA SHEET

MAX32591

DeepCover Secure Microcontroller with ARM926EJ-S Processor Core

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 contain detailed descriptions of device features and peripherals from a programming perspective.

- This MAX32591 data sheet, which contains electrical/timing specifications, package information, and pin descriptions.
- The MAX32591 revision-specific errata sheet.
- The MAX32591 User's Guide, which contains detailed information and programming guidelines for core features and peripherals.

Development and Technical Support

Technical support is available at **https://support.maximintegrated.com/micro**.

Ordering Information

PART	PACKAGE	JTAG	PRODUCTION SECURITY
MAX32591-LNS+*	228 CSBGA 11mm x 11mm 0.65mm pitch	No	Yes (Debug disabled)
MAX32591-LNJ+*	228 CSBGA 11mm x 11mm 0.65mm pitch	Yes	No (Prototype/ development)

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

**Not recommended for new designs.*

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.
228 CSBGA	X22811+1C	**21-100233**	**90-1000B81**

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/MAX32591** and click on **Request Full Data Sheet**.

For pricing, delivery, and ordering information, please visit Maxim Integrated's online storefront at https://www.maximintegrated.com/en/storefront/storefront.html.

