MAX32590

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 (MAX32590) provides an interoperable, secure, and cost-effective solution to build new generations of trusted devices such as multimedia-enabled portable EFT-POS terminals. The MAX32590 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 MAX32590 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 MAX32590 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 SD/SDHC/SDIO controller, 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 and thermal printer interface provide an integrated solution for mobile POS terminals. Additionally, a 3-channel, 10-bit ADC is provided for printer support and general use.

Applications

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

*For related parts and recommended products to use with this part, refer to **www.maximintegrated.com/MAX32590.related**.*

Features

- **ARM926EJ-S™ Processor Core with 16KB Data Cache and 32KB Instruction Cache**
- **384MHz Core Operating Frequency Through PLL (400MHz in Extended Frequency Mode)**
- **192MHz Multilayer AHB Bus Matrix (200MHz in Extended Frequency Mode)**
- **96MHz APB Bus Matrix (100MHz in Extended Frequency Mode)**
- **Security Features**
  - **Secure Bootloader with Public Key Authentication**
  - **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**
  - **256-Bit Flip-Flop-Based Nonvolatile AES Key Storage**
  - **Temperature and Voltage Tamper Monitor**
  - **Real-Time External Memory Encryption and Integrity Check**
  - **Real-Time Clock**
- **Memory**
  - **384KB System SRAM**
  - **4KB Instruction TCM, 4KB Data TCM**
  - **24KB AES User-Encryptable NV SRAM**
  - **Dual External Memory Controller (LPDDR400, SDRAM, SRAM, NOR Flash, NAND Flash)**
  - **2KB User-Programmable OTP**
  - **NAND Flash Controller with Hardware ECC**
- **Power Management**
  - **Flexible Clock Prescalers**
  - **Clock Gating Function**
  - **Low-Current Battery-Backup Operation**
  - **Configurable Low-Power Modes**

***Features** continued and **Ordering Information** appears at end of data sheet.*

***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**.*

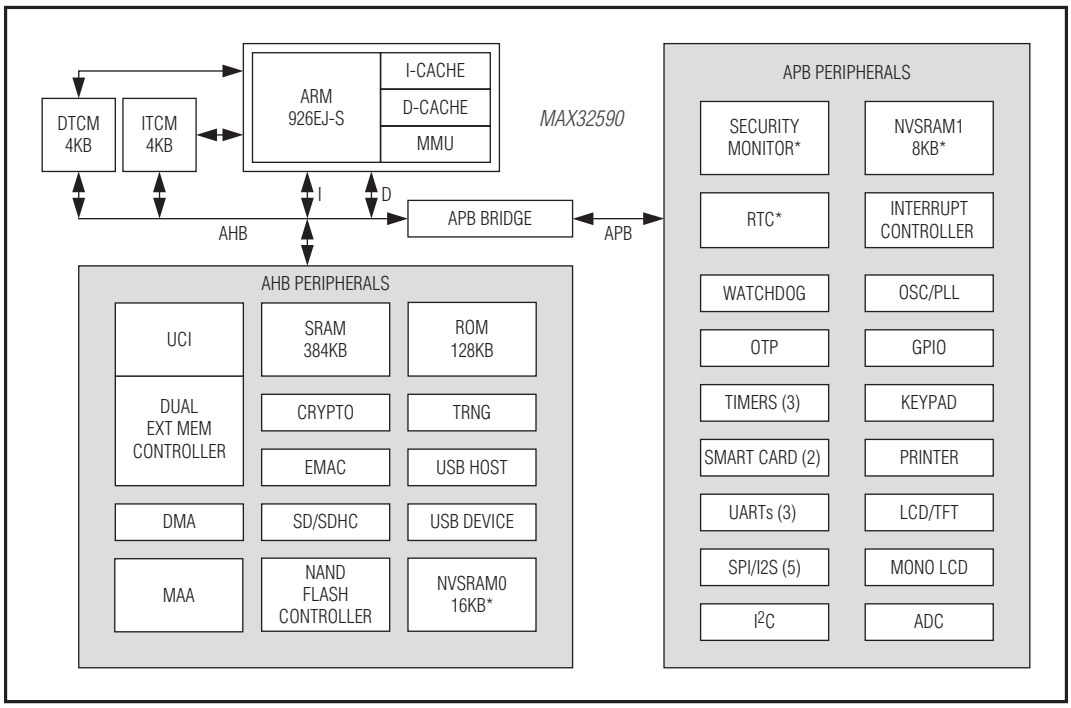
For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

19-6489; Rev 6; 10/16

MAX32590

DeepCover Secure Microcontroller with ARM926EJ-S Processor Core

Functional Diagram



*BATTERY-BACKED CIRCUITRY

MAX32590

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 MAX32590 data sheet, which contains electrical/timing specifications, package information, and pin descriptions.
- The MAX32590 revision-specific errata sheet.
- The MAX32590 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**.

Features (continued)

- **I/O and Peripherals**
  - **USB 2.0 Host/Device with Internal Transceivers**
  - **Three UART Ports/One I²C Port**
  - **Five SPI Ports with I²S Functionality**
  - **Two ISO 7816 Smart Card Interfaces**
  - **SD/SDHC/SDIO Interface**
  - **10/100Mbps Ethernet MAC Controller**
  - **Thermal Printer Interface**
  - **Three Timers with PWM Capability**
  - **Up to 160 General-Purpose I/O Pins**
  - **3-Channel, 10-Bit ADC**
  - **LCD Controller Supporting STN and TFT Displays**
  - **Monochrome LCD Controller**
  - **16-Channel DMA Controller**
  - **Advanced Interrupt Controller**

Ordering Information

PART	PACKAGE	JTAG	PRODUCTION SECURITY
MAX32590-LNS+*	324 CSBGA (15mm x 15mm)	No	Yes (Debug disabled)
MAX32590-L5S+	324 CSBGA (15mm x 15mm)	No	Yes (Debug disabled)
MAX32590-LNJ+*	324 CSBGA (15mm x 15mm)	Yes	No (Prototype/ development)
MAX32590-L5J+	324 CSBGA (15mm x 15mm)	Yes	No (Prototype/ development)

+Denotes 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.
324 CSBGA	X32455+1	21-0601	90-0392

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/MAX32590** and click on **Request Full Data Sheet**.

maxim integrated™

MAX32590

DeepCover Secure Microcontroller with ARM926EJ-S Processor Core

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	10/12	Initial release	—
1	5/13	Corrected the OTP size from 3KB to 2KB in the *General Description, Features,* and *Internal OTP* sections; corrected the CS[6:0} ball numbers in the *Bump Description* table; updated the MAA bullet under the *Cryptographic Accelerator* section to clarify it supports 4096-bit (CRT) RSA; removed references to RII (not supported) in the *Ethernet MAC* section; updated/renamed the *External Sensors* section to *External Tamper Sensors*	1, 10, 11, 16, 19, 20, 22
2	7/13	Added V_{CORE}, V_{BAT}, V_{IOM}, V_{IOS}, V_{DDA}, V_{USB} to the *Absolute Maximum Ratings* section, added V_{IOS}, V_{IOM}, and extended frequency mode parameters to the *Electrical Characteristics* table, and updated *Dual External Memory Controller* section	2, 4, 16
3	10/13	Replaced LFBGA references with CSBGA; corrected ball locations for SDDRCLK and SDDRCLKB in the *Bump Description*; clarified secure updates are also through SPI and that digital signature is used to verify bootloader transfer in the *Internal ROM and Bootloader* section; clarified difference between JTAG/non-JTAG device versions in the *JTAG Port* section; removed references to unsupported 32-bit LPDDR; updated EC table headers and notes with latest QA standard; removed unnecessary Note 6; changed $\overline{\text{MDDRCS}}$ and $\overline{\text{SDDRCS}}$ to active low in *Bump Configuration* and *Bump Description*	2–5, 7, 8, 11–13, 16, 23
4	3/15	Updated *Cryptographic Accelerator*, *SD Card Controller*, *Real-Time Clock (RTC)*, *Watchdog Timer*, and *Ordering Information* sections	4, 19–21, 23, 24
5	1/16	Renamed C2 ball, clarified BGR mode of 5:5:6, and updated *10-Bit ADC* and *Watchdog Timer* sections	5, 13, 18, 23
6	10/16	Updated *Features*, *USB*, and *Secure Keypad* sections	1, 18, 22

maxim integrated™