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 I2C 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**

<table>
<thead>
<tr>
<th>Applications</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Commerce</td>
<td>Secure Access Control</td>
</tr>
<tr>
<td>PCI Terminals</td>
<td>Secure Data Storage</td>
</tr>
<tr>
<td>PIN Pads</td>
<td>Pay-Per-Play</td>
</tr>
<tr>
<td>ATM Keyboards</td>
<td>Certificate Authentication</td>
</tr>
<tr>
<td>EMV Card Readers</td>
<td>Electronic Gaming</td>
</tr>
</tbody>
</table>

**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

For related parts and recommended products to use with this part, refer to www.maximintegrated.com/MAX32590.related. ARM926EJ-S is a trademark of ARM Limited. DeepCover is a registered trademark of Maxim Integrated Products, Inc.
MAX32590
DeepCover Secure Microcontroller with ARM926EJ-S Processor Core

Functional Diagram

AHB PERIPHERALS
- UCI
- DUAL EXT MEM CONTROLLER
- DMA
- MAA
- SRAM 384KB
- ROM 128KB
- CRYPTO
- TRNG
- EMAC
- USB HOST
- SD/SDHC
- USB DEVICE
- NAND FLASH CONTROLLER
- NVSRAM0 16KB*
- NVSRAM1 8KB*

APB PERIPHERALS
- SECURITY MONITOR**
- NVSRAM1 8KB*
- RTC*
- INTERRUPT CONTROLLER
- WATCHDOG
- OSC/PLL
- GPIO
- TIMERS (3)
- KEYPAD
- SMART CARD (2)
- PRINTER
- UARTs (3)
- LCD/TFT
- SPI/I2S (5)
- MONO LCD
- µC
- ADC

*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

<table>
<thead>
<tr>
<th>PART</th>
<th>PACKAGE</th>
<th>JTAG</th>
<th>PRODUCTION SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAX32590-LNS+*</td>
<td>324 CSBGA (15mm x 15mm)</td>
<td>No</td>
<td>Yes (Debug disabled)</td>
</tr>
<tr>
<td>MAX32590-L5S+</td>
<td>324 CSBGA (15mm x 15mm)</td>
<td>No</td>
<td>Yes (Debug disabled)</td>
</tr>
<tr>
<td>MAX32590-LNJ+*</td>
<td>324 CSBGA (15mm x 15mm)</td>
<td>Yes</td>
<td>No (Prototype/development)</td>
</tr>
<tr>
<td>MAX32590-L5J+</td>
<td>324 CSBGA (15mm x 15mm)</td>
<td>Yes</td>
<td>No (Prototype/ development)</td>
</tr>
</tbody>
</table>

+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.

<table>
<thead>
<tr>
<th>PACKAGE TYPE</th>
<th>PACKAGE CODE</th>
<th>OUTLINE NO.</th>
<th>LAND PATTERN NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>324 CSBGA</td>
<td>X32455+1</td>
<td>21-0601</td>
<td>90-0392</td>
</tr>
</tbody>
</table>

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.