# ABRIDGED DATA SHEET

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

## MAX32510

## DeepCover Secure Arm Cortex-M3-Based Flash Microcontroller

## 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 (MAX32510) provides an interoperable, secure, and cost-effective solution to build new generations of trusted devices. The MAX32510 includes an Arm® Cortex®-M3 core, 512KB of embedded flash, 96KB of system RAM, 1KB of battery-backed AES self-encrypted NVSRAM. It includes a cryptographic engine, a true random number generator, battery-backed RTC, environmental and tamper detection circuitry, and a smart card UART. It also includes a vast array of peripherals, such as I2C, USB, SPIs, UARTs, DMA, and ADC that add flexibility to control and differentiate the system design.

Thanks to its flexible architecture, the MAX32510 can be used as the main processor of an embedded device or as a coprocessor for applications that require more computing power. It can support the most frequent requirements for connected or standalone objects including secure key storage, secure boot, secure communications, certificates distribution and management as well as NVSRAM with instant content destruction capability which can support FIPS 140-2 level 3 or 4.

## Applications

- Card Readers
- Industrial Modules
- Embedded Communication Devices Such As Wireless Access Points
- IoT Nodes
- Gaming and Gambling Machines
- Voting Machines

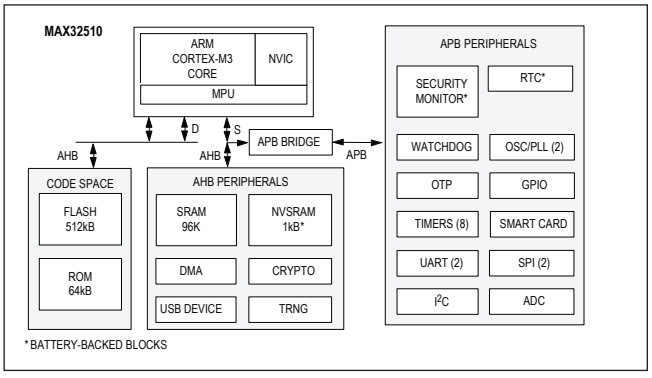
***Ordering Information* appears at end of data sheet.**



## Benefits and Features

- Arm Cortex-M3-Based Flash Microcontroller Allows for Easy Integration into Applications
  - 60MHz Core Operating Frequency Through PLL
  - 512KB Dual-Bank Flash Memory with Cache
  - 96KB System SRAM
  - 1KB AES Self-Encrypted NVSRAM
- Security Features Facilitate System-Level Protection
  - Secure Boot Loader with Public Key Authentication
  - AES, DES and SHA Hardware Accelerators
  - Modulo Arithmetic Hardware Accelerator (MAA) Supporting RSA, DSA, and ECDSA
  - Hardware True Random-Number Generator
  - Die Shield with Dynamic Fault Detection
  - 2 External Tamper Sensors with Independent Random Dynamic Patterns
  - Temperature and Voltage Tamper Monitor
  - Real-Time Clock
- Integrated Peripherals
  - One ISO 7816 Smart Card UART (without C4/C8)
  - USB 2.0 Device with Internal Transceiver
  - 2 SPI Ports, 2 UART Ports, and 1 I2C Controller
  - 8 Timers, All with PWM Capability
  - Up to 28 General-Purpose I/O Pins
  - 4-Channel, 10-Bit ADC
  - 4-Channel DMA Controller
- Power Management
  - Single 3.3V Supply Operation
  - Clock Gating Function
  - Low-Current Battery-Backup Operation

## Functional Diagram




*19-8783; Rev 3; 2/19*

Input clock is watched by the MAX32510 security mechanisms. The watchdog supports 16 programmable time delay periods with prescale values from $2^{16}$ to $2^{31}$. For system clock running at 60MHz, a maximum timeout delay of 35s is supported.

### JTAG Port

The JTAG interface is used for code loading, ICE debug activities and for control of Boundary Scan activities. The ordering information section contains unique part numbers for devices with the JTAG interface enabled or disabled. Devices with the JTAG interface enabled are used during application development and debugging. Devices with the JTAG interface disabled prevent access to the debugging interface and should be used in mass production. For more Information, refer to the Secure ROM User Guide.

### 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 MAX32510 data sheet, which contains electrical/timing specifications, package information, and pin descriptions.
- The MAX32510 revision-specific errata sheet.
- The MAX32510 User 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 | PIN-PACKAGE | ICE |
|---|---|---|
| MAX32510-DPS+ | 68 TQFN (8mm x 8mm, 0.40mm pitch) | No |
| MAX32510-DPS+T | 68 TQFN (8mm x 8mm, 0.40mm pitch) | No |
| MAX32510-BNJ+ | 68 TQFN (8mm x 8mm, 0.40mm pitch) | Yes |
| MAX32510-BNS+ | 68 TQFN (8mm x 8mm, 0.40mm pitch) | No |
| MAX32510-BNS+T | 68 TQFN (8mm x 8mm, 0.40mm pitch) | No |

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

T *=Tape and reel.*