ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

MAX32555

DeepCover Secure Cortex-M3 Flash Microcontroller

General Description

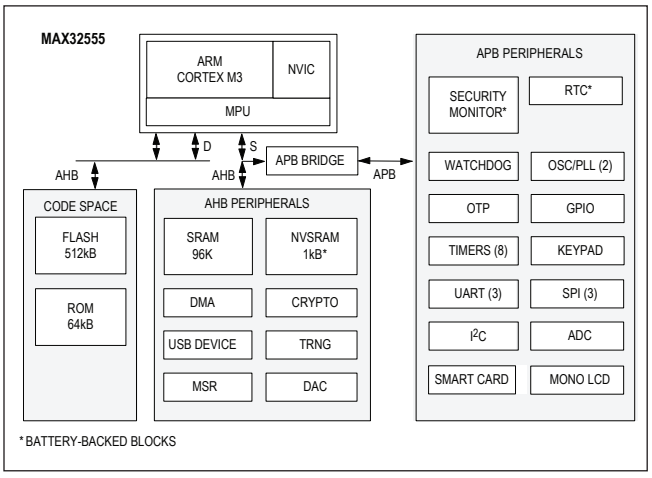
DeepCover® embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The DeepCover Secure microcontroller (MAX32555) provides an interoperable, secure, and cost-effective solution to build new generations of trusted devices such as mobile chip and pin pads. The MAX32555 is based on a Cortex M3 processor with 512KB of embedded flash, 96KB of system RAM, 1KB of battery-backed AES self-encrypted NVSRAM. It includes all the essential functions of mobile POS terminal including a cryptographic engine, a true random number generator, battery-backed RTC, environmental and tamper detection circuitry, a magnetic stripe reader, a smart card controller with embedded transceiver to directly support 1.8V, 3.3V, and 5V cards, and an integrated secure keypad controller. It also includes a vast array of peripherals, SPIs, UARTs, DMA, ADC, and DAC that add flexibility to control and differentiate the system design.

Applications

- PCI Mobile Payment Terminals (mPOS)
- ATM Keyboards
- EMV Card Reader

Functional Diagram



Benefits and Features

- ARM® Cortex® M3 Processor Core 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
  - 8-Line Secure Keypad Controller
  - Hardware True Random-Number Generator
  - Die Shield with Dynamic Fault Detection
  - 4 External Tamper Sensors with Independent Random Dynamic Patterns
  - 256-Bit Flip-Flop-Based Battery-Backup AES Key Storage
  - Temperature and Voltage Tamper Monitor
  - Real-Time Clock
- Integrated Peripherals Reduce External Component Count
  - Triple-Track Magnetic Stripe Head Interface
  - One ISO 7816 Smart Card Interface with Integrated Transceiver (1.8V, 3V, and 5V)
  - USB 2.0 Device with Internal Transceiver and Dedicated PLL
  - 3 SPI Ports, 3 UART Ports, and 1 I^2C Controller
  - 8 Timers, All with PWM Capability
  - Up to 70 General-Purpose I/O Pins
  - 6-Channel, 10-Bit ADC and 1-Channel, 8-Bit DAC
  - Monochrome LCD Controller
  - 4-Channel DMA Controller
- Power Management Optimizes Battery Life and Reduces Active Power Consumption
  - Single 3.3V Supply Operation*
  - Integrated Battery-Backup Switch
  - Clock Gating Function
  - Low-Current Battery-Backup Operation

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

**5V smart card support requires external 5.0V supply.*

19-7654; Rev 2; 5/17

maxim integrated™