# ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

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

## MAX32558

## DeepCover Secure Arm Cortex-M3 Flash Microcontroller

## General Description

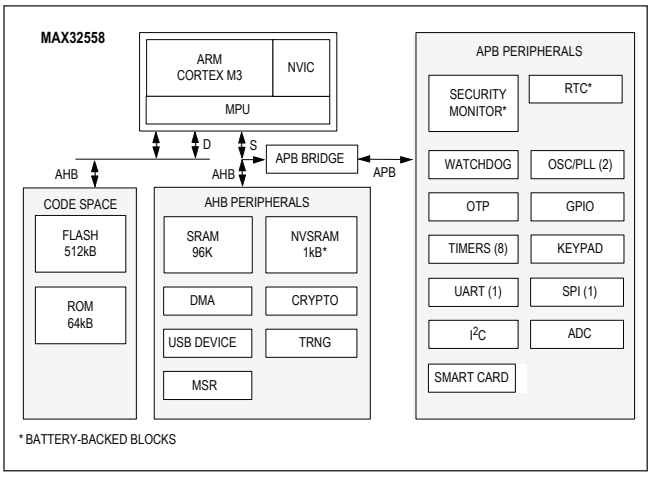
DeepCover® embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

The MAX32558 is based on an Arm® Cortex®-M3 processor with 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, 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, USB SPIs, UARTs, DMA, and ADC that add flexibility to control and differentiate the system design.

## Applications

- PCI Mobile Payment Terminals (mPOS)
- ATM Keyboards
- EMV Card Readers
- Standalone Smartcard Readers
- HSMs
- Industrial Modules

## 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
  - 4x3 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
  - 1 SPI Port, 1 UART Port, and 1 $I^2C$ Controller
  - 8 Timers, with up to 2 PWM I/O
  - Up to 27 General-Purpose I/O Pins
  - 1-Channel, 10-Bit ADC
  - 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.*



*19-100098; Rev 4; 2/19*

maxim integrated™

# Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

Maxim Integrated:

MAX32558/W+U