maxim integrated™

DS3640

DeepCover Security Manager with I²C Interface and 1KB Nonimprinting Battery-Backed Encryption Key SRAM

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 Security Manager (DS3640) is a secure supervisor with 1024 bytes of SRAM for applications requiring the secure storage of encryption keys, including POS terminals. The DS3640 supports the highest security level requirements of the FIPS 140.2, Common Criteria, PCI PED, and EMV® 4.1 certification agencies. The 1KB key memory is constantly complemented in the background to prevent oxide stress and memory imprinting. In the event of a qualified tamper event, the key memory is rapidly cleared.

The device includes a real-time clock (RTC), CPU supervisor, watchdog timer, and on-chip temperature sensor. In the event of a primary power failure, an external battery source is automatically switched in to keep the key memory, RTC, and tamper-detection circuitry active. The DS3640 provides low-leakage tamper-detection inputs for interface to external sensors, interlocks, and anti-tamper meshes. The DS3640 will also invoke a tamper event if the backup battery drops below a specified threshold, absolute temperature or temperature rate-of-change exceeds programmed limits, or crystal-oscillator frequency falls outside a specified window. The tamper event is latched and time stamped for future debugging purposes.

Access to the RTC, tamper monitoring, key memory, and device configuration is conducted through an I²C-compatible interface. The DS3640 is assembled in a Pb-free CSBGA package, which enhances key security in that the leads are not exposed to the outer edges of the package.

Applications

Point-of-Sale Terminals

Gaming

Routers/Switches

IT Security

Alarm Systems

DeepCover is a registered trademark of Maxim Integrated Products, Inc.

EMV is a registered trademark of EMVCo LLC.

Features

- **1024-Byte Nonimprinting Key Memory with High-Speed Erase**
- **64-Byte General-Purpose RAM (Not Cleared)**
- **Real-Time Clock with Leap Year Compensation Valid Up to 2100**
- **Watchdog Timer**
- **CPU Supervisor**
- **Four General-Purpose Tamper-Detect Comparators with Associated Reference**
- **Three Tamper-Detect Logic Inputs**
- **On-Chip Programmable Temperature Sensing with Proprietary Rate-of-Change Detector**
- **On-Chip Random Number Generator (RNG)**
- **Latching and Time Stamping of Tamper Events**
- **Crystal Oscillator Tamper Monitoring**
- **Low Power Consumption**
- **3.0V to 3.6V Single-Supply Operation**
- **CSBGA Package with No Horizontally Exposed Leads**

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS3640B+	-40°C to +85°C	25 CSBGA
DS3640B+TRL	-40°C to +85°C	25 CSBGA

+Denotes a lead(Pb)-free/RoHS-compliant package.
TRL = Tape and reel.

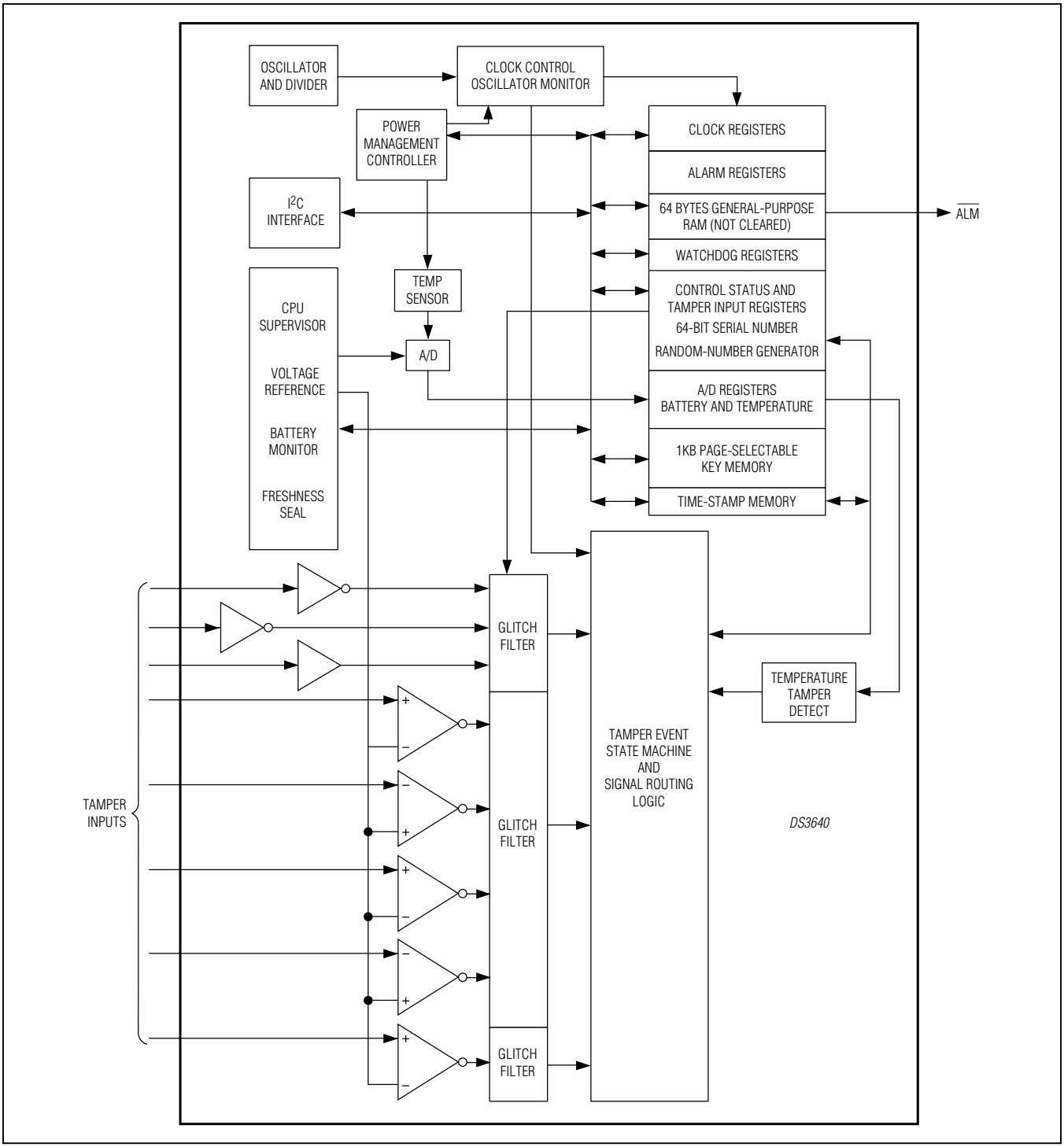
For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

119-0008; Rev 9; 9/13

DS3640

DeepCover Security Manager with I²C Interface and 1KB Nonimprinting Battery-Backed Encryption Key SRAM

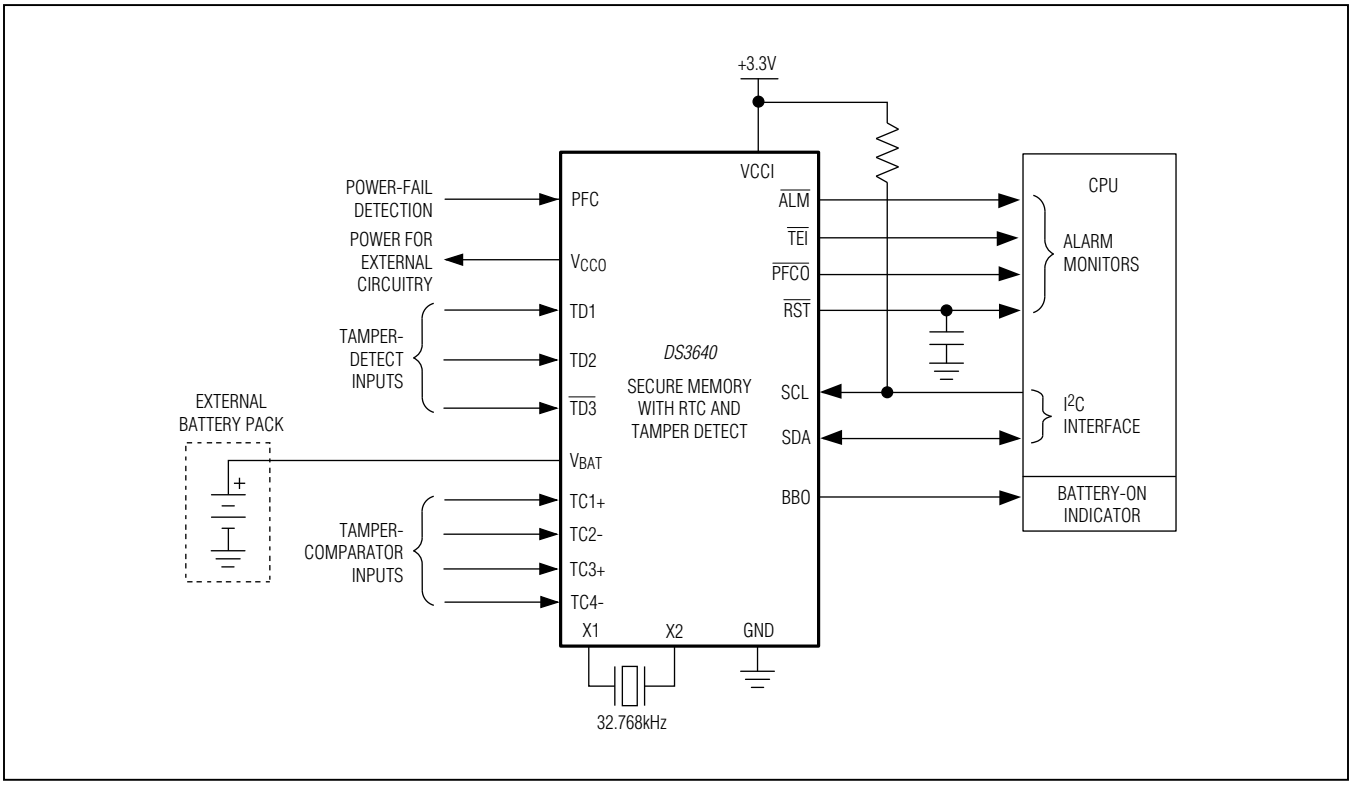
Functional Diagram



DS3640

DeepCover Security Manager with I²C Interface and 1KB Nonimprinting Battery-Backed Encryption Key SRAM

Typical Operating Circuit



Package Information

For the latest package outline information and land patterns (footprints), go to **www.maximintegated.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.
25 CSBGA	X25+2	21-0361	90-0298

Mouser Electronics

Authorized Distributor

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

Maxim Integrated:

DS3640B+