DS3644

DeepCover Security Manager with 1KB Secure Memory and Programmable Tamper Hierarchy

Tamper-Detection Hierarchy with On-Chip Nonimprinting Memory Safeguard Critical Data

NDA Required. Request Full Data Sheet Subscribe Active in Production.

Please check latest availability status for a specific part variant.

OVERVIEW | PARAMETRIC SPECS | DESIGN RESOURCES | QUALITY AND ENVIRONMENTAL | ORDER

Related Resources

RELATED PACKAGING

TECHNICAL DOCS

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 (DS3644) is a secure supervisor with 1024 bytes of SRAM for the secure storage of sensitive data and the physical tamper-sensing response functions required in cryptographic processors and data security equipment.

One of the DS3644's primary features is the on-chip nonimprinting memory, consisting of eight 128-byte banks incorporating a high-speed, direct-wired clearing function. The 1KB memory is constantly complemented in the background to prevent memory imprinting of data. The DS3644 architecture allows the user to clear selective banks of the memory based upon specified tamper events. In the event of a qualified tamper event, the desired bank(s) of memory are rapidly cleared and a negative bias can be applied to erase external memory.

The DS3644 includes a seconds counter, watchdog timer, CPU supervisor, nonvolatile (NV) SRAM controller, and on-chip temperature sensor. In the event of a primary power failure, an external battery source is automatically switched in to keep the memory, time, and tamper-detection circuitry active. The DS3644 provides low-leakage, tamper-detection inputs for interface to external sensors, interlocks, and antitamper meshes. The DS3644 also invokes a tamper event on absolute temperature, if the temperature rate-of-change exceeds programmed limits, or if the crystal oscillator frequency falls outside a specified window. The tamper event is latched and timestamped for fault-recovery purposes.

Access to the timer, tamper monitoring, memory, and device configuration is conducted through an I²C-compatible interface. The DS3644 is assembled in a Pb-free, 7mm x 7mm x 0.8mm CSBGA package.

Key Features

- Memory
  - 1024-Byte Nonimprinting Memory with High-Speed Erase
  - 64 Bytes General-Purpose RAM (Not Cleared)
  - External SRAM Control and Optional Tamper-Event Erasure
  - Segmented Tamper-Detection Memory Hierarchy with Programmable Tamper-Event Sources
- Tamper
  - On-Chip Programmable Temperature Sensing with Proprietary Rate-of-Change (ROC) Detector
  - Two General-Purpose Tamper-Detect Logic Inputs
  - Four Uncommitted Tamper-Detect Comparator Inputs
  - Four Window Comparators with On-Chip Reference Voltage

Applications/Uses

- Access-Control Security Systems
- ATMs
- Cryptographic Processors
- E-Commerce Servers
- Gaming Systems
- Network Routers and Switches
- Network Storage Servers
- PIN Pads
- Point-of-Sale Terminals
- Secure Communications

- Latching and Timestamping of Tamper Events
- Crystal Oscillator Tamper Monitoring

- Other
  - Programmable Power-Consumption Options for Very Low Standby Current
  - 64-Bit Unique Silicon Serial Number
  - On-Chip Random-Number Generator (RNG)
  - 32-Bit Seconds Counter with Watchdog Timer and Alarm Output
  - CPU Supervisor
  - I^2C-Compatible Interface

- Set-Top Boxes
- Smart Card Readers
- Software-Defined Radios