DS3645

4KB Secure Memory with Tamper Protection for Network Server Applications

Single-Chip Solution Integrates Advanced Physical Security with On-Chip Encryption Key Memory

NDA Required. Request Full Data Sheet

Description

The DS3645 is a secure supervisor with 4096 bytes of SRAM for applications requiring the secure storage of sensitive data and the physical tamper-sensing response functions required in cryptographic processors and data security equipment.

One of the DS3645's primary features is the on-chip encryption key memory, consisting of 32 128-byte banks incorporating a high-speed, direct-clearing function. The 4KB key memory is constantly complemented in the background to prevent memory imprinting. In the event of a qualified tamper event, the key memory is rapidly cleared and a negative bias is applied to clear SRAM external to the DS3645.

The device includes a real-time 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 key memory, seconds counter, and tamper-detection circuitry active. The DS3645 provides low-leakage tamper-detection inputs for interface to external sensors, interlocks, and antitamper meshes. The DS3645 also invokes a tamper event if the backup battery drops below a specified threshold or 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 future debugging purposes.

Access to the seconds counter, tamper monitoring, key memory, and device configuration is conducted through an I^2-C-compatible interface. The DS3645 is assembled in a CSBGA package, which enhances key security because the leads are not exposed to the outer edges of the package.

Key Features

- 4096-Byte Nonimprinting Key Memory with High-Speed Erase
- Optional External SRAM Clear Upon Qualified Tamper Event
- 64-Byte General-Purpose RAM (Not Cleared)
- 32-Bit Seconds Counter
- Watchdog Timer
- CPU Supervisor
- Four General-Purpose Tamper-Detect Comparators
- Four Window Comparators with On-Chip Reference Voltages
- Two Tamper-Detect Logic Inputs
- On-Chip, Programmable Temperature Sensing with Proprietary Rate-of-Change Detector
- On-Chip Random-Number Generator (RNG)
- Latching and Timestamping of Tamper Events
- Crystal Oscillator Tamper Monitoring
- Low-Power Consumption
- Wide Temperature Range: -55°C to +95°C
- CSBGA Package (7mm x 7mm x 0.8mm) with No Horizontally Exposed Leads
- I^2C-Compatible Interface

Applications/Uses

- Alarm Systems
- Gaming
- IT Security
- Point-of-Sale Terminals
- Routers/Switches

Part Number	Analog Voltages Monitored	Digital Inputs Monitored	Internal Key Memory (Bytes)	Package/Pins	Oper. Temp. (°C)
DS3645	12	4	4096	CSBGA/49	-55 to +95

Part Number	Status	Carrier Type	Package
DS3645B+	Active	Tray	CSBGA; 49Pin; 49mm^2;
DS3645B+TRL	Active	Reel	CSBGA; 49Pin; 49mm^2;
DS3645K	Active	Box	
DS3645B-TRL	NLA	Reel	CSBGA; 49Pin; 49mm^2;
DS3645B	Active	Tray	CSBGA; 49Pin; 49mm^2;
DS3645B-W+	NLA	Tray	CSBGA; 49Pin; 49mm^2;