maxim integrated™

MAX36025

DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption

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 (MAX36025) is a highly integrated device intended to address the security requirements of high-end cryptographic systems and data-at-rest storage applications. The device employs a tamper-reactive dual AES cryptographic engine architecture that facilitates the cost effective implementation of multiple cipher channels across compartmentalized system nodes and storage elements.

Two SPI interfaces and one generic Serial Flash interface are provided for secure, flexible communication to external system nodes. The MAX36025 can be programmed to route any of these interface inputs through one, both, or neither of the dual AES engines, and also to any of these interface outputs.

Device programming and configuration are performed through an I²C-compatible interface. The I²C interface can be secured using an integrated authentication protocol for an additional layer of security regarding validation of ancillary system elements as well as FoF (friend or foe) decisions. Additionally, the MAX36025 can encrypt I²C communications using a configurable AES key.

The MAX36025 includes on-chip nonimprinting memory that incorporates a high-speed, direct-wired clearing function. The memory is constantly complemented in the background to prevent memory imprinting of data. The MAX36025 architecture allows the user to clear selective banks of the memory based upon specified tamper events. In the event of a qualified tamper, the desired bank(s) of memory are rapidly cleared and a negative bias can be applied to erase external memory.

The MAX36025 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 MAX36025 provides low-leakage, tamper-detection inputs for interfacing to external sensors, interlocks, and antitamper meshes. The MAX36025 also invokes a tamper event on absolute temperature, if the temperature exceeds programmed limits, or if the crystal oscillator frequency falls outside of a specified window. The tamper event is latched and time-stamped for fault recovery purposes.

The hardwired AES engine implementation and extensive suite of tamper detection and response mechanisms make the MAX36025 well suited across a wide range of applications where consistent security policies must be maintained.

Features

- **Cryptographic**
  - **Triple Mode Encryption: AES-ECB, AES-CTR, AES-CBC**
  - **Dual Encryption Cores to Allow Dual Key Cipher Translation and Routing**
  - **On-Chip Secure Key Storage**
  - **Pipelined Dual Asynchronous Bidirectional SPI Data Ports**
- **Storage**
  - **1K x 8 On-Chip Nonimprinting Memory with High-Speed Tamper-Reactive Erase**
  - **External Serial Flash Interface**
  - **Tamper-Reactive NV SRAM Controller**
- **Authentication**
  - **On-Chip Pseudorandom Number Generator with Internal Seed**
  - **I²C Control Interface Requires Authentication Through AES Encryption**
- **Tamper Detection and Response**
  - **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**
  - **Latching and Timestamping of Tamper Events**
  - **Crystal Oscillator Tamper Monitoring**
- **Differential Power Analysis and TEMPEST Countermeasures**
  - **On-Chip Spread-Spectrum Clock Source for the AES Cores and the External Memory Interface**
  - **Power Controller Ensures Constant Current During Cryptographic Operations**
- **Underwriters Laboratories (UL) Recognized**

Applications

Secure Communications
Software-Defined Radios
Cryptographic Processors
e-Commerce Servers
Network Storage Servers
Network Routers and Switches
Access-Control Security Systems
Point-of-Sale Terminals
PIN Pads
ATMs
Smart Card Readers
Set-Top Boxes
Casino Gaming Systems

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

For related parts and recommended products to use with this part, refer to: www.maximintegrated.com/MAX36025.related

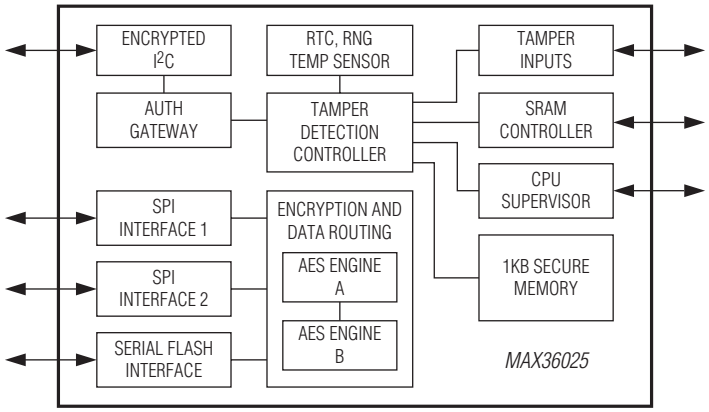
For pricing, delivery, and ordering information, please contact Maxim Direct at 1-888-629-4642, or visit Maxim Integrated's website at www.maximintegrated.com.

119-0018; Rev 1; 5/13

MAX36025

DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption

Functional Diagram



System Diagram