Data Sheet

DS28E15

DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM

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 Secure Authenticator (DS28E15) combines crypto-strong bidirectional secure challenge-and-response authentication functionality with an implementation based on the FIPS 180-3-specified Secure Hash Algorithm (SHA-256). A 512-bit user-programmable EEPROM array provides nonvolatile storage of application data. Additional protected memory holds a read-protected secret for SHA-256 operations and settings for memory protection control. Each device has its own guaranteed unique 64-bit ROM identification number (ROM ID) that is factory programmed into the chip. This unique ROM ID is used as a fundamental input parameter for cryptographic operations and also serves as an electronic serial number within the application. A bidirectional security model enables two-way authentication between a host system and slave-embedded DS28E15. Slave-to-host authentication is used by a host system to securely validate that an attached or embedded DS28E15 is authentic. Host-to-slave authentication is used to protect DS28E15 user memory from being modified by a unauthentic host. The DS28E15 communicates over the single-contact 1-WireM bus at overdrive speed. The communication follows the 1-Wire protocol with the ROM ID acting as node address in the case of a multi-device 1-Wire network.

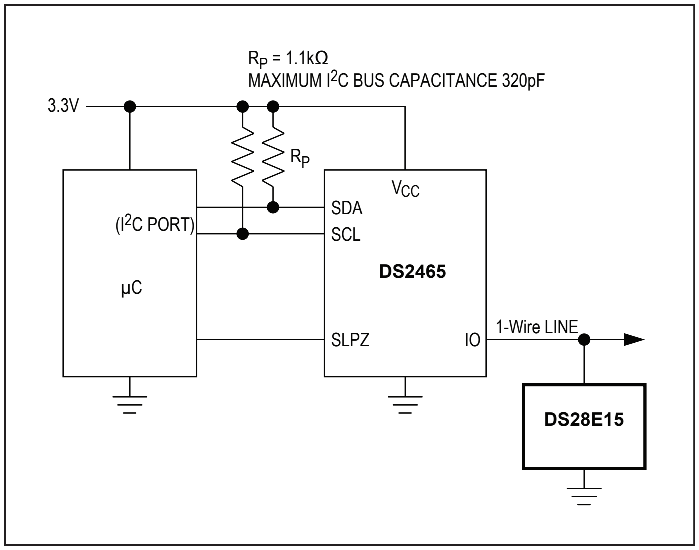
Applications

- Authentication of Consumables
- Secure Feature Control

Benefits and Features

- 512-Bit EEPROM with SHA-256 Authentication for Reads and Writes
  - Symmetric-Key-Based Bidirectional Secure Authentication Model Based on SHA-256
  - Strong Authentication with a High-Bit-Count User-Programmable Secret and Input Challenge
  - 512 Bits of User EEPROM Partitioned Into Two Pages of 256 Bits
  - User-Programmable and Irreversible EEPROM Protection Modes Including Authentication, Write and Read Protect, and OTP/EPROM Emulation
  - Unique Factory-Programmed, 64-Bit Identification Number
- Minimalist 1-Wire Interface Lowers Cost and Interface Complexity
  - Reduces Control, Address, Data, Power, and Programming Signals to a Single Data Pin
  - ±8kV HBM ESD Protection (typ)
  - 2-Pin SFN, 6-Pin TDFN-EP, and 6-Pin TSOC Packages
  - Operating Range: 3.3V ±10%, -40°C to +85°C

Typical Application Circuit



DeepCover is a trademark and 1-Wire is a registered trademark of Maxim Integrated Products, Inc.

Visit Web Support to complete the nondisclosure agreement (NDA) required to receive additional product information.

Information furnished by Analog Devices is believed to be accurate and reliable. However, no responsibility is assumed by Analog Devices for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implicationor otherwise under any patent or patent rights of Analog Devices. Trademarks andregistered trademarks are the property of their respective owners.