

**DeepCover Secure Authenticator****General Description**

The DS28C36 is a DeepCover® secure authenticator that provides a core set of cryptographic tools derived from integrated asymmetric (ECC-P256) and symmetric (SHA-256) security functions. In addition to the security services provided by the hardware implemented crypto engines, the device integrates a FIPS/NIST true random number generator (RNG), 8Kb of secured EEPROM, a decrement-only counter, two pins of configurable GPIO, and a unique 64-bit ROM identification number (ROM ID).

The ECC public/private key capabilities operate from the NIST defined P-256 curve and include FIPS 186 compliant ECDSA signature generation and verification to support a bidirectional asymmetric key authentication model. The SHA-256 secret-key capabilities are compliant with FIPS 180 and are flexibly used either in conjunction with ECDSA operations or independently for multiple HMAC functions.

Two GPIO pins can be independently operated under command control and include configurability supporting authenticated and nonauthenticated operation including an ECDSA-based crypto-robust mode to support secure-boot of a host processor.

DeepCover embedded security solutions cloak sensitive data under multiple layers of advanced security to provide the most secure key storage possible. To protect against device-level security attacks, invasive and noninvasive countermeasures are implemented including active die shield, encrypted storage of keys, and algorithmic methods.

**Applications**

- IoT Node Crypto-Protection
- Accessory and Peripheral Secure Authentication
- Secure Storage of Cryptographic Keys for a Host Controller
- Secure Boot or Download of Firmware and/or System Parameters

**Benefits and Features**

- ECC-256 Compute Engine
  - FIPS 186 ECDSA P256 Signature and Verification
  - ECDH Key Exchange with Authentication Prevents Man-in-the-Middle Attacks
  - ECDSA Authenticated R/W of Configurable Memory
- FIPS 180 SHA-256 Compute Engine
  - HMAC
- SHA-256 OTP (One-Time Pad) Encrypted R/W of Configurable Memory Through ECDH Established Key
- Two GPIO Pins with Optional Authentication Control
  - Open-Drain, 4mA/0.4V
  - Optional SHA-256 or ECDSA Authenticated On/Off and State Read
  - Optional ECDSA Certificate to Set On/Off after Multiblock Hash for Secure Boot
- RNG with NIST SP 800-90B Compliant Entropy Source with Function to Read Out
- Optional Chip Generated Pr/Pu Key Pairs for ECC Operations
- 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
- 8Kbits of EEPROM for User Data, Keys, and Certificates
- Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - Optional Input Data Component to Crypto and Key Operations
- I<sup>2</sup>C Communication Up to 1MHz
- Operating Range: 2.2V to 3.63V, -40°C to +85°C
- 6-Pin TDFN Package

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

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

Rev. 3

**DOCUMENT FEEDBACK**

**TECHNICAL SUPPORT**

*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 implication or otherwise under any patent or patent rights of Analog Devices. Trademarks and registered trademarks are the property of their respective owners.*

