DEEPCOVER SECURE AUTHENTICATORS

ECDSA, HMAC SHA-256, ECDH and Secure Boot Asymmetric and Symmetric Crypto Security Functions (I²C or 1-Wire Interface)

PRODUCT DESCRIPTION

The **DS28C36** (I²C) and **DS28E36** (1-Wire®) DeepCover Secure Authenticators provide a set of asymmetric-key and symmetric-key cryptographic tools in a low-cost and compact solution. Asymmetric public-key features are supported with P256-based elliptic-curve (ECC) algorithm and a symmetric secret-key with SHA-256. These devices are fully flexible in terms of operational configuration and public-key vs. secret-key feature usage. End-application use cases include bidirectional authentication, secure storage of system data (for example systems crypto keys), secure verification of system-critical data, secure boot, and secure use control. Additionally, two pins of GPIO are provided with optional, secure state control and level sensing. In addition to cryptographic strength, these devices provide protection against invasive and noninvasive security attacks with technologies including active die shield, encrypted storage of keys, and algorithmic methods. The **DS2476** is a companion co-processor to both the DS28C36 and DS28E36 for applications where the host system microcontroller has insufficient computing resources for ECC algorithms or required secure storage for a SHA-256 symmetric key.

KEY FEATURES

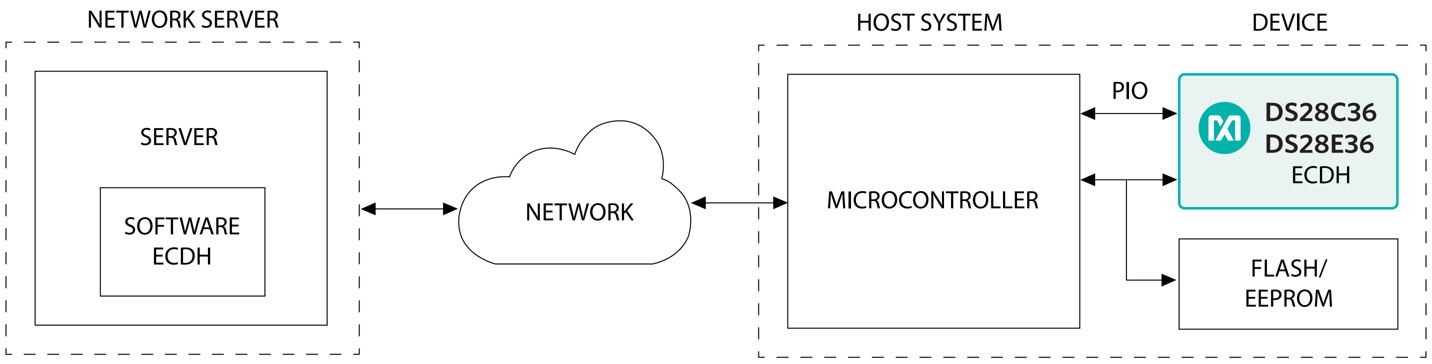
- ECC-256 Compute Engine
  - FIPS 186 ECDSA P256 Signature and Verification for Bidirectional Authentication and Optional GPIO Control
  - Diffie-Hellman (ECDH) Key Establishment to Communicate Secure Host-System Data
  - Configurable ECDSA Authenticated R/W of Memory
- SHA-256 Compute Engine
  - FIPS 198 HMAC for Bidirectional Authentication and Optional GPIO Control
  - FIPS 180 MAC for Secure Download/Boot Operations
- SHA-256 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 On/Off State Setting to Enhance Secure Download/Boot Operations
- 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
- 8Kb of EEPROM for User Data, Keys, and Certificates
- Unique and Unalterable Factory-Programmed 64-Bit Identification Number (ROM ID)
- 100kHz and 400kHz I²C Communication
- 11.7kbps and 62.5kbps 1-Wire Communication
- Operating Range: 3.3V ±10%, -40°C to +85°C
- 6-Pin TDFN Package

APPLICATION BENEFITS

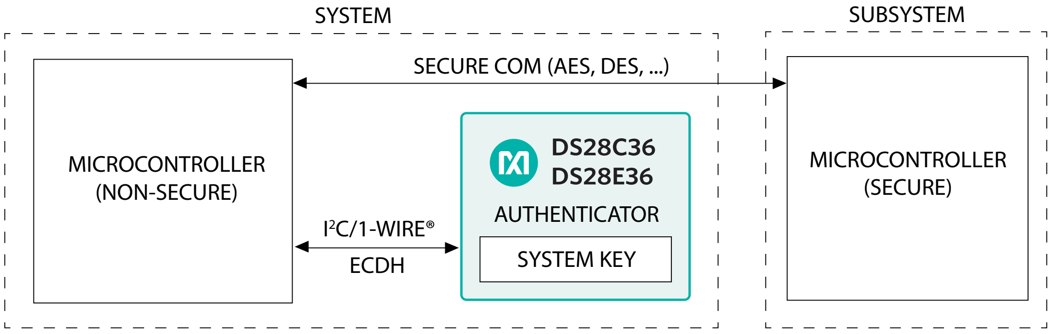
- Protect R&D investment by preventing aftermarket counterfeits
- For off-chip use, securely store and retrieve system crypto-keys
- Authenticate device peripherals and network-attached equipment
- Securely control or sense external actuators or sensors
- Tamper proof memory for calibration, usage, and/or expiration data
- Securely verify system data downloads or provide secure boot operations

TYPICAL BLOCK DIAGRAMS

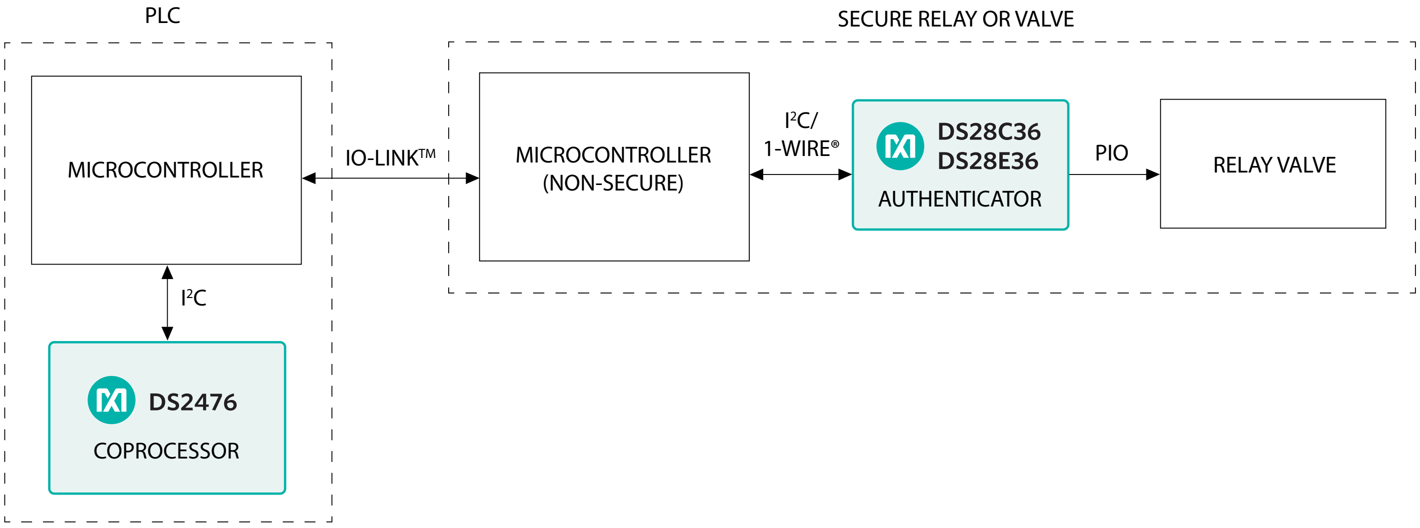
IoT Node Protection Using ECDH Key Establishment and Secure Boot



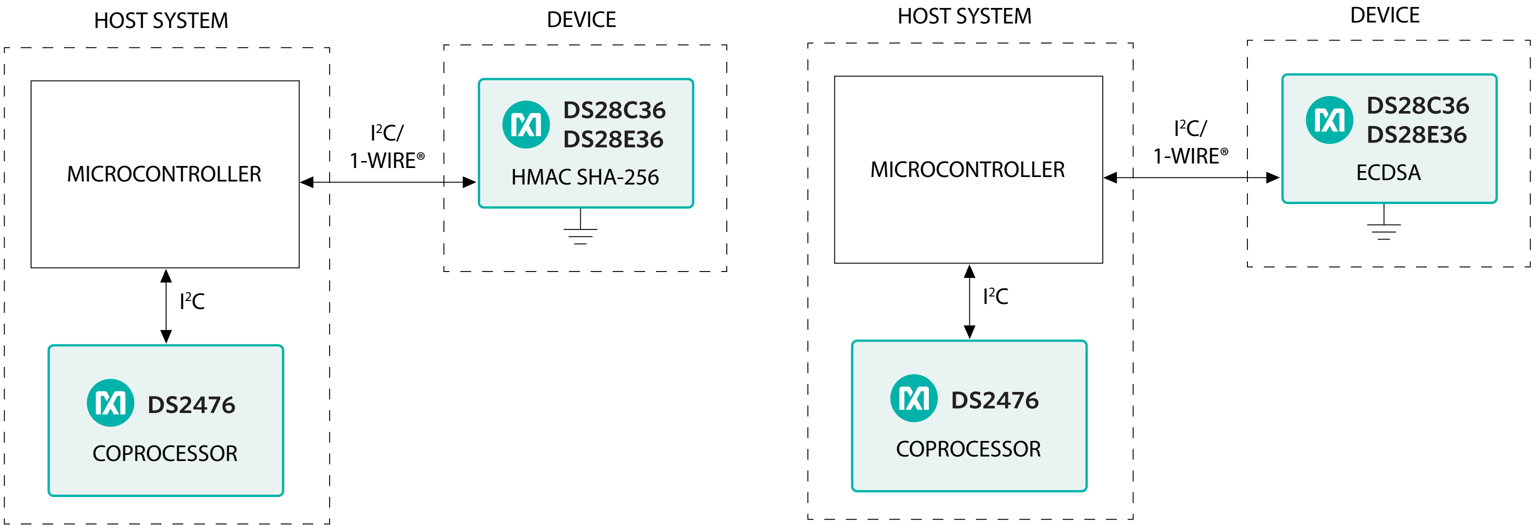
Secure System Key Storage



Industrial Secure Smart Sensor



IP Protection Using HMAC SHA-256 or ECDSA Authentication



FOCUS PRODUCTS

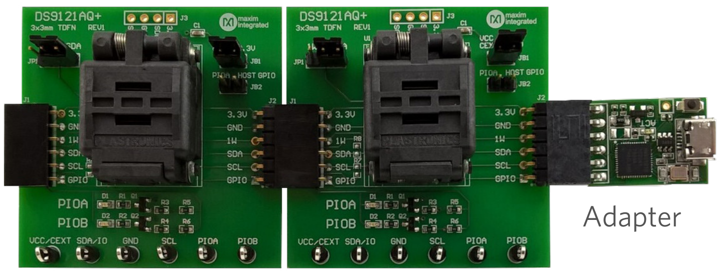
Base Part	Type	Interface	EEPROM	Package Options	Evaluation Kit	Order
DS28C36	Authenticator	I^{2}C	*8Kb	TDFN	DS28C36EVKIT	🛒
DS28E36		1-Wire			DS28E36EVKIT	🛒
DS2476	Coprocessor	I^{2}C			Included	🛒

*User and key storage memory total

SOFTWARE RESOURCE SELECTION GUIDE

Evaluation Kit	Coprocessor Implementation	Platform	Resource Library
DS28C36EVKIT	DS2476 (IC)	PC	DS28C36EVKIT GUI
			DS28E36EVKIT GUI
DS28E36EVKIT	DS2476 (IC)	Microcontroller	DS28C36_DS2476_C-Lib
			DS28E36_DS2476_C-Lib
	C-Library		DS28C36_SW-CoPro_C-Lib
			DS28E36_SW-CoPro_C-Lib

RELATED RESOURCES



- Secure Authenticators
- DS28C36EVKIT: Evaluation Kit for DS28C36 and DS2476
- DS28E36EVKIT: Evaluation Kit for DS28E36 and DS2476
- DeepCover Secure Authenticators
- DeepCover Embedded Security Solution Guide