DEEPCOVER SECURE AUTHENTICATORS

ECDSA Asymmetric Crypto Security with ChipDNA PUF Protection

PRODUCT DESCRIPTION

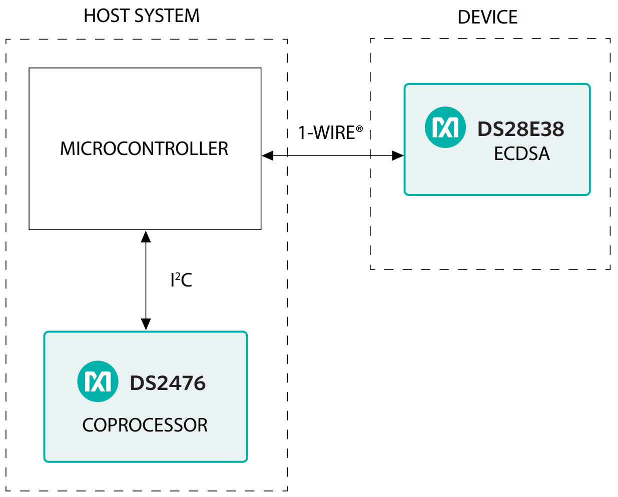
Our ChipDNA™ physically unclonable function (PUF) technology provides unsurpassed protection against security attacks and an optional component to ECDSA operation. ChipDNA technology uses the random variation of fundamental MOSFET device characteristics that naturally occur during wafer fabrication to generate unique cryptographic keys that are repeatable over time, temperature, and operating voltage. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, preventing discovery of the unique value used by the chip cryptographic functions.

The **DS28E38** DeepCover® Secure Authenticator with ChipDNA Protection provides asymmetric-key cryptographic authentication in a low-cost and compact solution. Asymmetric public-key features are supported with the P256-based elliptic-curve (ECC) algorithm. The DS28E38 utilizes the ChipDNA output as key content to cryptographically secure all device stored data and optionally, under user control, as the private key for the ECDSA signing operation. In addition to cryptographic strength, the device provides protection against invasive and noninvasive security attacks with technologies that include active die shield, encrypted storage of keys, and algorithmic methods. End application use cases include device authentication, secure IoT node and message authentication, reference design license management, and secure use control of consumables. The **DS2476** is a companion coprocessor to the DS28E38 for applications where the host system microcontroller has insufficient computing resources for ECC algorithms.

KEY FEATURES

- Robust Countermeasures Protect Against Security Attacks
  - ChipDNA Prevents Attacks to Discover Keys and Secures Device Data
  - Actively Monitored Die Shield Detects and Reacts to Intrusion Attempts
  - All Stored Data Cryptographically Protected from Discovery
- ECC-256 Compute Engine
  - FIPS 186 ECDSA P256 Signature for Challenge/Response Authentication
  - Options for ECDSA Public/Private key Pair Source Include ChipDNA-Generated, Chip-Computed, and User-Installed
- RNG with NIST SP 800-90B Compliant Entropy Source with Function to Read Out
- 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
- 2Kb of EEPROM for User Data, Keys, and Certificates
- Unique and Unalterable Factory-Programmed 64-Bit Identification Number (ROM ID)
- Single-Contact, 1-Wire® Interface Communication with Host at 11.7kbps and 62.5kbps
- Operating Range: 3.3V ±10%, -40°C to +85°C
- 6-Pin TDFN Package (3mm x 3mm)

TYPICAL BLOCK DIAGRAM



IP Protection Using ECDSA Signature Challenge/Response Authentication

APPLICATION BENEFITS

- Protect R&D investment by preventing aftermarket counterfeits
- Authenticate device peripherals and network-attached equipment
- Tamper proof memory for calibration, manufacturing, and/or expiration data
- Securely manage limited use consumables

FOCUS PRODUCTS

Base Part	Type	Voltage (V)	EEPROM	Package Options	Evaluation Kit	Order
DS28E38	Authenticator	3.3	2Kb*	TDFN	DS28E38EVKIT	🛒
DS2476	Coprocessor		8Kb*			🛒

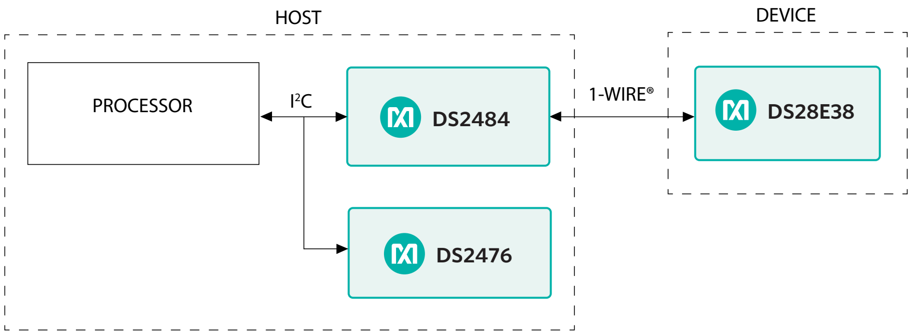
*User and key storage memory total

SOFTWARE RESOURCE SELECTION GUIDE

Evaluation Kit	Coprocessor Implementation	Platform	Resource Library
DS28E38EVKIT	DS2476 (IC)	PC	DS28E38EVKIT GUI
		Microcontroller	DS28E38_DS2476_C-Lib
	C-Library		DS28E38_SW-CoPro_C-Lib

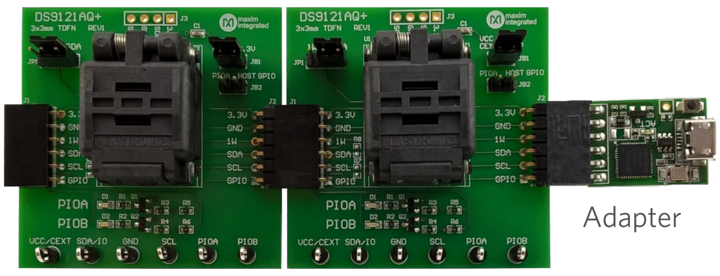
MAXREFDES168 SOFTWARE REFERENCE DESIGN

The MAXREFDES168 demonstrates authentication of the DS28E38 DeepCover Secure ECDSA Authenticator with ChipDNA PUF protection, the companion DS2476 secure coprocessor, and the DS2484 1-Wire master, in an embedded Arm®-based environment. The included Eclipse project is configured for immediate use on Maxim's MAX32625MBED evaluation board, with Arm-enabled devices also supported. All source code, including authentication examples and drivers for the DS28E38, DS2476, and DS2484 conform to the ISO C++98 standard for maximum portability between compilers.



Hardware Implementation of the MAXREFDES168

RELATED RESOURCES



DS28E38 DS2476 Adapter

Secure Authenticators

DS28E38EVKIT: Evaluation Kit for DS28E38 and DS2476

DeepCover Secure Authenticators

DeepCover Embedded Security Solution Guide