ABRIDGED DATA SHEET

MAXQ1061

DeepCover Cryptographic Controller for Embedded Devices

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 cryptographic controller (MAXQ1061) protects the confidentiality, authenticity and integrity of software IP, communication and revenue models. It is ideal for connected embedded devices, industrial networking, PLC, and network appliances.

The embedded, comprehensive cryptographic toolbox provides key generation and storage up to full SSL/TLS/DTLS support by offering a high level of abstraction including TLS/DTLS key negotiation, ECDSA-based TLS/DTLS authentication, digital signature generation and verification, SSL/TLS/DTLS packet encryption, and MAC algorithms. It can also serve as a secure bootloader for an external generic microcontroller.

32KB of user-programmable EEPROM securely store certificates, public keys, private and secret keys, monotonic counters, and arbitrary data. A flexible file system manages access rights for the objects. The device is controlled over a SPI or I^2C interface. Life cycle management and a secure key loading protocol are provided.

Cryptographic algorithms supported by the device include AES, ECC, ECDSA signature scheme, SHA, and MAC digest algorithms. The true random number generator can be used for on-chip key generation. A separate hardware AES engine over SPI, allows it to function as a coprocessor for stream encryption.

The advanced physical, environmental and logical protections, are designed to meet the stringent requirements of FIPS and Common Criteria EAL4+ certifications.

Applications

- Smart Metering
- Certificate Distribution and Management
- Secure Access Control
- Electronic Signature Generation
- Cybersecurity for Critical Infrastructures

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

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

Benefits and Features

- Advanced Cryptographic Tool Box Seamlessly Supports Highly Secure Key Storage
  - Certificates Chain Management
  - Secure 32KB File System Based on Nonvolatile EEPROM (500K Cycles) for Extensive Key and Certificate Storage
  - Symmetric-key: AES-128/-256 (ECB, CBC, CCM)
  - Asymmetric-key: ECC NIST P-256, -521, -384
  - Secure Hash: SHA-256, -384, -512
  - MAC Digest: CBC-MAC, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512
  - Signature Schemes: ECDSA (FIPS 186-4)
  - Key Exchange: EC Diffie-Hellman (TLS)
  - 128-Bit AES Stream Encryption Engine Over SPI (up to 20Mb/s) Supporting AES-GCM and AES-ECB Modes
  - On-Chip Key Generation: ECC, AES
  - Random Number Generation: True RNG
- High-Level Functions Simplify SSL/TLS/DTLS Implementations
  - TLS/DTLS Key Negotiation (PSK, ECDH, ECDHE)
  - ECDSA Based TLS/DTLS Authentication, Digital Signature Generation and Verification
  - SSL/TLS/DTLS Packet Encryption (AES)
  - MAC Algorithm (HMAC-SHA256)
- Extensive Host/System Services Increase Flexibility and Reduce System Cost
  - Watchdog Timer
  - Power-On Reset/Brownout Reset
  - Secure Boot Function
  - Tamper Detection
  - Life Cycle Management and Key Loading Protocol
  - Flexible File System With User-Programmable Access Conditions for Each Object Software Reset
  - Software Reset, Shutdown, and Wake-Up Functions
- Multiple Communication Interface Options for Simpler Connection to a Host Processor
  - I^2C Slave Controller
  - SPI Slave Controller with a Dedicated DMA Channel and 128-Bit AES Stream Encryption Engine Supporting AES-GCM and AES-ECB Modes

19-8718; Rev 0; 11/16

maxim integrated™

Detailed Description

The DeepCover cryptographic controller (MAXQ1061) is an effective and easy to implement solution for strengthening security in embedded systems.

A comprehensive cryptographic toolbox supports an array of security needs. Simpler systems may require as little as the provided key generation and storage. For high levels of security, full SSL/TLS/DTLS support offers a high level of abstraction.

Cryptographic algorithms supported by the device include AES-128/-256 with support for ECB, CBC, and CCM modes, ECC (up to NIST P-521), ECDSA signature scheme, SHA-2 (up to SHA-512) secure hash algorithms, MAC digest algorithms such as CBC-MAC or HMAC-SHA.

It also has provision for on-chip key generation based upon a random number generator. The device also provides a separate hardware AES engine over SPI, supporting AES-GCM and AES-ECB modes, and that can be used to off-load a host processor for stream encryption.

Communication Interface Selection

The device communicates through the I²C or SPI bus, determined by the application (TLS toolbox or AES-SPI).

TLS/DTLS Cryptographic Toolbox

The comprehensive cryptographic toolbox simplifies and increases the security and resistance of SSL/TLS/DTLS based applications It offers a high level of abstraction for the following functions:

- Offloads the TLS key exchange
- Securely stores certificates (makes them immutable)
- Securely stores private keys
- Helps securely verifying certificates and certificate revocation lists
- Securely authenticates to the other peer
- Performs the key exchange securely
- Can encrypt/decrypt and sign/verify data during execution of the TLS record protocol using the keys negotiated during the TLS handshake
- TLS key exchange and TLS record encryption/decryption are performed internally and never exposed. The master secret can be exported to perform the TLS record processing externally.

The above security features prevent:

- The use of rogue certificates. Certificates are internally verified and are managed using a dedicated administrator authentication only. TLS handshake cannot be performed with an unverified certificate.
- The exposure of private keys used for authenticating the equipment embedding the MAXQ1061. Hardware resistance prevents the disclosure of such private keys.
- The exposure of the TLS sensitive data (shared secret or session keys). These data remain inside the security module.

AES-SPI Engine

The 128-bit AES engine supports AES-GCM (SP 800-38D compliant) and AES-ECB (SP 800-A compliant) modes. A dedicated register enables key transfer from the TLS toolbox to the AES SPI engine. The block is tightly connected to the SPI slave controller through a dedicated DMA controller providing high-speed encryption/decryption of a data stream coming over the SPI interface.

The SPI controller provides a dedicated command interpreter that can only be used when in AES-SPI mode. The command interpreter includes the following command set:

- Authentication only mode
- Encryption only mode
- Encryption with authentication mode
- AES operation mode selection
- Keys and initialization vector (IV) loading protocol
- Secure storage and handling of block cipher key (EK) and authentication key (AK)
- Software reset
- Shutdown

SSL/TLS/DTLS Functions

- TLS/DTLS key negotiation (ECDH, ECDHE)
- ECDSA-based TLS/DTLS authentication, digital signature generation and verification
- SSL/TLS/DTLS packet encryption (AES)
- MAC algorithm (HMAC-SHA256)
- SSL/TLS/DTLS host stack for most CPU architectures

TLS/DTLS Cipher Suites

- RFC 5487 preshared key (TLS)
  - TLS_PSK_WITH_AES_128_GCM_SHA256
  - TLS_PSK_WITH_AES_256_GCM_SHA384
  - TLS_PSK_WITH_AES_128_CBC_SHA256
  - TLS_PSK_WITH_AES_256_CBC_SHA384
- RFC 6655 AES-CCM (TLS)
  - TLS_PSK_WITH_AES_128_CCM
  - TLS_PSK_WITH_AES_256_CCM
  - TLS_PSK_WITH_AES_128_CCM_8
  - TLS_PSK_WITH_AES_256_CCM_8

- RFC 5489 ECDHE_PSK (TLS)
  - TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
- RFC 5289 AES-CBC/GCM ECC (TLS)
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 7251 AES-CCM ECC (TLS)
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM
  - TLS_ECDHE_ECDSA_WITH_AES_256_CCM
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
  - TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8

Cryptographic Services

- Symmetric-key algorithms: AES-128/-256 (ECB, CBC, CCM)
- Asymmetric-key: ECC NIST P-256, -521, -384
- Secure hash algorithms: SHA-256, -384, -51
- MAC digest algorithms: CBC-MAC, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512
- Signature schemes: ECDSA (FIPS 186-4)
- Key exchange algorithms: EC Diffie-Hellman (TLS)
- On-chip key generation: ECC, AES
- Random number generation: True RNG

System Services

- Life cycle management and key loading protocol
- Software reset
- Shutdown command

Secure Channel

TLS and DTLS protect the data during transmission between endpoints. The optional secure channel provides confidentiality with the host processor by supporting AES-CBC, and integrity using AES-CBC-MAC. Secure messaging performs a key exchange, and those keys sign and encrypt the commands and the responses using AES.

True Random Number Generator

The IC provides a hardware-based true random number generator.

Watchdog Timer

The MAXQ1061 can act as an external watchdog timer (WDT) for a host microcontroller. When enabled, the WDI pin must be toggled within the user-configurable timeout period. Failure to toggle the pin within the timeout period results in a WDT timeout. A WDT timeout can assert a RESET_OUT pulse if enabled. A timeout does not cause an internal reset.

Tamper Detection

Multiple tamper detection features ensure the security of information contained within the MAXQ1061. The security features are independently enabled and can assert a RESET_OUT pulse if enabled.

Secure Boot

The integrity of the host processor's data and code can be verified through the hash and signature verification mechanisms. Object access can be configured after a successful secure boot.

Life Cycle Management

A managed life cycle changes functions and properties over time, as shown in Table 2. At each state of the one-way life cycle, the device and parties are granted initialization, read or modification rights to specific information.

TLS/DTLS Host Stack

The SSL/TLS/DTLS stack supports TLS1.2/DTLS 1.2, in client mode. In this stack, security sensitive processing is deported into the MAXQ1061. Therefore, the TLS host stack does not need to manipulate or store sensitive/secret data.

The TLS host stack uses the ARM® mbed™ TLS.

32KB Secure EEPROM Storage

32KB of secure EEPROM is accessible in TLS toolbox mode. Data objects can be volatile or not and can be stored in the nonvolatile memory. To be resistant to power loss during write operations, the object modification is atomic. Key objects are stored in an integrity-protected manner and can never be read in the clear. They are automatically verified before use. Key pairs should be generated internally and stored in a persistent key pair object. Key pairs can also be generated externally and imported after successful signature verification using an import public key present in the module. Arbitrary key pairs cannot be used; verification is mandatory.

Certificate Storage

Certificates are stored in an integrity-protected manner. They are automatically verified and trusted using one or more parent certificates in the certification chain (certificates already stored in the IC). The device verifies the digital signature of the certificates and can extract their public key.

Arbitrary certificates cannot be stored; verification by a parent certificate or by a dedicated public key is mandatory.

Serial Peripherals

SPI

The serial peripheral interface (SPI) is provided in the SPI-AES and TLS (SPI) modes. SPI is a four-wire bus providing fast, synchronous, full-duplex communication between the IC and the host system. The peripheral provides the following features:

- Slave mode operation
- Active-low SSEL
- Characters transmitted LSB first
- Data protocol uses SPI Mode 0

I²C

The I²C bus is provided in the TLS (I²C) mode. It is a bidirectional, two-wire serial bus that provides a medium-speed communications network. It can operate as a one-to-one, one-to-many, or many-to-many communications medium. It provides the following features:

- Slave mode operation
- Maximum I²C bit rate of 400kps (fast mode)
- Default address of 0x60 can be configured
- Supports standard (7-bit) addressing
- Supports I²C clock stretching

Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
MAXQ1061EUD+	-40°C to +109°C	14 TSSOP
MAXQ1061EUD+T	-40°C to +109°C	14 TSSOP

+Denotes a lead(Pb)-free/RoHS-compliant device.

T = Tape and reel.

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.

