DEEPCOVER®
EMBEDDED SECURITY

Solution Guide

Featuring ChipDNA™ Physically Unclonable Function Technology

www.maximintegrated.com/DeepCover

maxim integrated™

Table of Contents

Synopsis

Advanced Hardware-Based Technologies for Optimal Performance and Strength

Our world is getting more connected every day. However, the Internet of Things (IoT) revolution will only be successful if users can trust connected objects and the underlying infrastructure. In the past, security was a concern only for dedicated applications such as electronic payment systems. Today, security has become a requirement in many additional applications such as smart grid, process control, and building automation.

At the same time, malicious hackers have become more sophisticated, collaborating through online communities and building advanced attack scenarios to infiltrate IoT devices. Consequently, designers of electronic devices face new challenges. Not only must they implement very robust security against sophisticated attacks, they must also optimize their research and development efforts while keeping BOM costs low. This is where Maxim's security expertise excels.

MAXIM'S HISTORY OF SECURITY

Figure 1. The Technology Foundation of DeepCover Security

Maxim has been providing security to the IoT market since long before the term "IoT" was even coined. We designed the first secure microcontroller and have continued to invest in digital security design for the last 30 years. Our solutions for point-of-sale (POS) terminals, securing the confidentiality and integrity of data to the cloud, have been a cornerstone of our offering. Based on this experience, we offer a comprehensive portfolio of secure microcontrollers and secure authentication ICs capable of meeting the security challenges of tomorrow (Figure 1).

Given our long experience securing embedded systems, we understand that ICs alone cannot solve all of a designer's challenges. Beyond silicon, we provide reference schematics, drivers, middleware, communication stacks and support to enable fast time-to-market. Our system approach also guarantees a higher security level. Our ability to provide secure factory programming and key management brings great peace of mind to our customers and is unequalled in our industry.

UNPRECEDENTED SECURITY PROTECTION WITH ChipDNA

Leveraging analog IC design and device physics expertise, we have developed a patented physically unclonable function (PUF) solution, known as ChipDNA, to elevate the security strength of our DeepCover products at an industry-leading level. With ChipDNA, the naturally occurring random characteristics of CMOS transistors are utilized to generate a high-quality cryptographic key that is unique to each IC. Critically important, the PUF-generated key is repeatable over temperature, voltage, and operating life conditions of the IC.

ChipDNA technology brings an exponential increase in protection against the invasive and reverse-engineering attacks that hackers apply when attempting to break the security. Attempts to probe or observe ChipDNA operation modifies the underlying circuit characteristics, preventing the discovery of the unique value used by the chip cryptographic functions. Similarly, more exhaustive reverse-engineering attempts are defeated due to the factory conditioning required to make the PUF circuitry operational. The per-device unique key is generated by the PUF circuitry only when needed for cryptographic operations and then instantaneously deleted. Most importantly, the ChipDNA key never resides statically in registers or memory, nor does it ever leave the electrical boundary of the security IC.

In addition to the protection benefits, ChipDNA simplifies or eliminates the need for secure IC key management. For example, the PUF-generated key is used directly for functions including:

- Root key for derived key operations
- Symmetric secret to encrypt/decrypt data stored in the nonvolatile memory of the secure IC
- Private key for ECDSA signature generation
- Private key for ECDH key establishment

DEEPCOVER SOLUTIONS FOR EMBEDDED SECURITY

Embedded systems are susceptible to numerous threats, including:

- Counterfeiting
- Hardware or software IP reverse engineering
- Malware injection or firmware substitution
- Eavesdropping
- Identity theft
- Unauthorized network connection
- Unauthorized re-use

Secure device authentication, secure boot, and encryption are the answers to these attacks. DeepCover Secure Authenticators and DeepCover Secure Microcontrollers incorporate these techniques to ensure your platforms are trustworthy.

Trusted platforms, IP protection, secure download, and secure communication are the most frequent requirements for IoT node security. Table 1 maps our DeepCover solutions to common IoT needs.

DEEPCOVER SECURE AUTHENTICATORS

Secure Authenticators provide a core set of fixed-function crypto operations, secure key storage, and numerous supplemental feature options including: secure download/boot processing,

Table 1. DeepCover Security Solutions for IoT Security Needs

Requirements		DeepCover Secure Authentication ICs		DeepCover Secure Microcontrollers
		SHA-Based	ECDSA-Based	
Trust	Device authentication	✓	✓	✓
	Usage control/features enablement	✓	✓	✓
	Secure boot/download		✓	✓
IP Protection	Hardware and firmware anticloning	✓	✓	✓
	Firmware encryption			✓
Secure Communications	Certificate distribution and verification		✓	✓
	Packet encryption	✓	✓	✓
	Full TLS support			✓
	Small message encryption	✓	✓	✓

protected nonvolatile memory for end application use, secure GPIO, decrement-only counters, session key generation, true random number source, and encrypted R/W of stored data. In addition to cryptographic strength, secure authenticators provide advanced physical protection to address malicious die-level security attacks including ChipDNA on newer generation devices. As the inventor of the revolutionary 1-Wire® interface, Maxim is a leader in the development of devices that connect to nontraditional form-factors such as printer cartridges, medical disposables and battery packs.

Secure Authenticator Applications

Maxim's secure authentication solutions solve a wide range of security issues including:

Common Application Requirements

- Product Quality/Safety
- Counterfeit Prevention
- Secure Download/Boot
- Use/Feature Control
- IoT Device Integrity/Authenticity

Solved with Targeted Product Features

- Bidirectional Authentication
- Secure System Data Storage
- Secure Use Counting
- System Session Key Generation
- Secure Memory Settings
- Secure GPIO
- Random Number Source

ECDSA Authenticators

The **DS28E38** is an ECDSA authenticator that incorporates ChipDNA technology. The device utilizes the ChipDNA output as key content to cryptographically secure all device-stored data. Optionally, it is under user control as the private key for the ECDSA signing operation. With ChipDNA capability, the device provides a core set of cryptographic tools derived from integrated blocks including an asymmetric (ECC-P256) hardware engine, a FIPS/NIST-compliant true random number generator (TRNG), 2Kb of secured EEPROM, a decrement-only counter, and a unique 64-bit ROM identification number (ROM ID). The ECC public/private key capabilities operate from the NIST-defined P-256 curve to provide a FIPS 186-compliant ECDSA signature generation function.

The **DS28C36** and the companion **DS2476** provide a core set of asymmetric-key and symmetric-key cryptographic tools in a compact, low-cost solution. Asymmetric public-key features are supported with the FIPS 186 P256-based elliptic-curve (ECC) algorithm and symmetric secret-key with FIPS 180/198 SHA-256 HMAC. The 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, system 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.

Table 2. DeepCover ECDSA Authentication Devices

Part Number	Type	Interface*	User EEPROM	Package Option
DS28E38	Authenticator with ChipDNA	1-Wire	2kb	TDFN
DS28C36	Authenticator	I²C	4kb	TDFN
DS2476	Coprocessor	I²C	4kb	TDFN
DS28E35	Authenticator	1-Wire	1kb	TSOC, TDFN
DS2475	Coprocessor	I²C/1-Wire	—	SOT

**All parts operate at 3.3V ±10%.*

The DS2476 is a companion coprocessor to the DS28C36 and DS28E38 for applications where the host system microcontroller has insufficient computing resources for ECC algorithms or lacks the required secure storage for a ECDSA private key or SHA-256 system secret, when used.

Table 2 lists our DeepCover ECDSA authenticators and companion coprocessors.

SHA-256 Authenticators

The **DS28E15**/**DS28E22**/**DS28E25** family of devices operate with the 1-Wire interface and offer several options for user-memory size and operating voltage. The **DS2465** is a companion coprocessor with integrated 1-Wire line driver which provides secure storage for a system SHA-256 key. All devices provide a FIPS 180 based bidirectional authentication capability. The **DS28C22** offers the SHA-256 functionality with an I²C interface.

The **MAX66240**/**MAX66242** are NFC/RFID transponders with SHA-256 bidirectional authentication. The MAX66242 expands this functionality with an option for RF energy harvesting, an I²C interface that can be configured as master or slave, and one GPIO pin. The **MAX66300** is a host system NFC transceiver and companion SHA-256 coprocessor to the transponders and provides secure storage for SHA-256 system keys.

Table 3 lists our DeepCover SHA-256 authentication ICs, companion co-processors, transceivers, and responders.

Table 3. DeepCover SHA-256 Authentication Devices

Part Number	Type	Interface	Operating Voltage	User EEPROM	Package Options
DS28C22	Authenticator	I²C	3.3V	3kb	TDFN
DS2465	Coprocessor	I²C/1-Wire	3.3V	0.5kb	TSOC
DS28E15				0.5kb	SFN, TSOC, TDFN
DS28E22	Authenticator	1-Wire	3.3V	2kb	TSOC, TDFN
DS28E25				4kb	SFN, TO92, TSOC, TDFN
DS24L65	Coprocessor	I²C/1-Wire		0.5kb	TSOC
DS28EL15			1.8V	0.5kb	SFN, TDFN
DS28EL22	Authenticator	1-Wire		2kb	TDFN
DS28EL25				4kb	TDFN
MAX66240	Authenticator Transponder	NFC	Passive	4kb	SOIC, TDFN, 8-Bump WLP
MAX66242		NFC/I²C	Passive (optional 3.3V)		
MAX66300	Coprocessor Transceiver	NFC/UART/SPI	3.3V, 5V	1kb	TQFN

Computing, Peripherals, & Cables | Internet of Things | Medical Consumables

Figure 2. Secure Authentication Applications Made Possible by 1-Wire

The 1-Wire Interface

Maxim's 1-Wire interface solution provides a versatile, rugged and very reliable interconnect method for secure authentication in areas not previously possible. This is of particular value when there is a contact limited interconnect to the subassembly that needs authentication. In addition to IoT nodes, examples include medical sensors and tools, pluggable modules, industrial controllers, authentication for printer cartridges and general IP protection. Figure 2 provides examples of end applications that 1-Wire enables.

1-Wire Product Features:

- Single Contact Sufficient for Control and Operation
- Power Derived from the 1-Wire Bus ("Parasite Power")
- Unique ID Factory-Programmed into Each Device
- Multidrop Capable: Supports Multiple Devices on a Single Line
- Exceptional ESD Performance, typically 8kV HBM

Tools and Services for Secure Authenticators

Reference Designs:

- **MAXREFDES155**: Embedded Security in IoT - Public-Key Secured Data Paths with ECDSA (Figure 3)
- **MAXREFDES143**: IoT Authenticated Sensing and Notification with SHA-256
- **MAXREFDES43**: Xilinx® Zynq® ZedBoard™ Authentication with DS28C22 SHA-256
- **MAXREFDES44**: Xilinx Zynq MicroZed™ Authentication with DS28E35 ECDSA
- **MAXREFDES34**: Xilinx Spartan®-6 Authentication with DS28E15 SHA-256

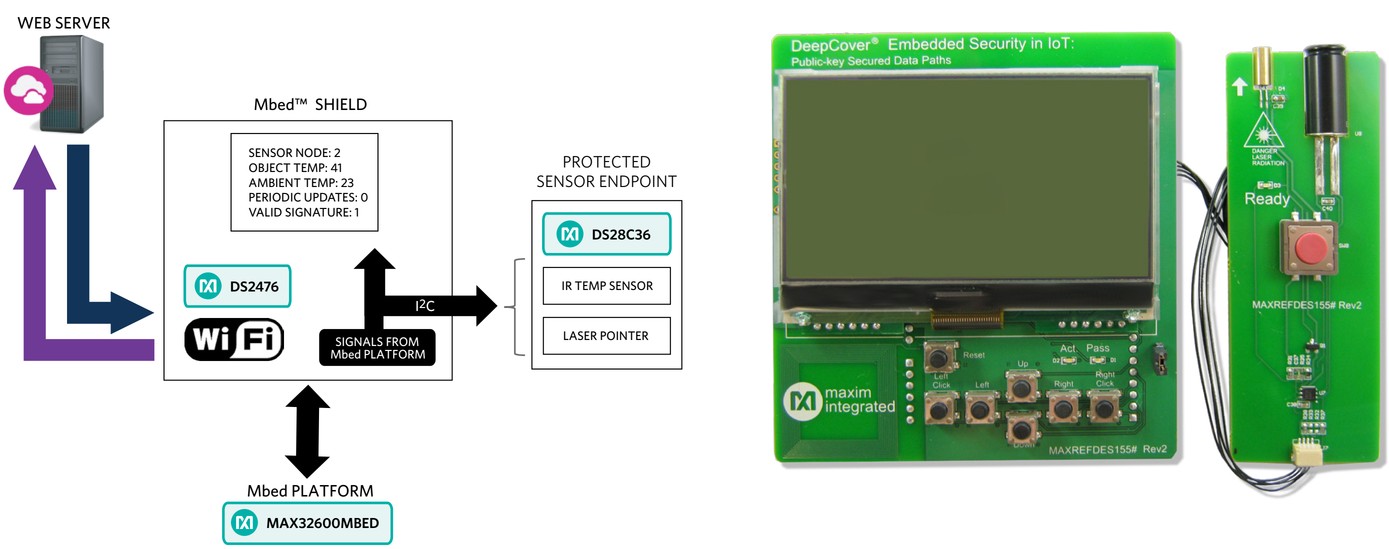

Figure 3. MAXREFDES155 Reference Design

Factory Key Management Service for Secure Authenticators

A fundamental cryptosystem principle regarding keys that was introduced in 1883 by Dutch cryptographer Auguste Kerckhoffs applies equally today:

> *"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."*

With this in mind, OEMs that use secure authenticators in their end applications must ensure that their keys are programmed prior to equipment being delivered to end customers and that the keys are not compromised at any point in the supply chain. As a value-add option to OEMs, Maxim offers a key management and programming service to securely install keys, certificates, and application data prior to product shipment. Our secure process for transferring your data to our factory includes an encrypted file transfer of device settings from your computer to our production environment. You can be assured that the secret or private key is not compromised during manufacturing or at any point in the supply chain. Contact your local Maxim distributor, representative, or account executive for additional information.

Secure Authenticator Evaluation Kits

Table 4 lists the evaluation kits for each secure authenticator device.

Secure Multi-Device Programmer

Although factory, OEM and distributor programming services are geared towards high-volume production builds, there is also a need for security when building prototypes and for low-volume applications. The **DS9488-GP8** multi-device programming system securely install keys, data, and device configuration settings for a variety of our 1-Wire and I²C interfaced products. The system optionally enables encrypted programming files to be securely moved from one programmer to another to support development at one location and programming at another, if needed. Socket adapters are available for most device packages.

DEEPCOVER SECURE MICROCONTROLLERS

In the 1990s, Maxim designed the DS5200, the first secure microcontroller. Since then, we have continued to invest in developing industry-leading security features to face future challenges.

DeepCover Secure Microcontrollers for Embedded Security

Maxim pioneered active tamper reaction technology, which instantaneously wipes out the keys and secrets of devices during attempted tampering, enabling a security level of FIPS 140-2 level 3 or 4.

Active tamper reaction technology requires a battery to operate. For end-products and applications that cannot accommodate a battery, we developed the DeepCover secure cryptographic controller, **MAXQ1061**, which is based on tamper-proof EEPROM and does not require a battery (Figure 4). Table 5 lists DeepCover secure microcontrollers designed specifically for embedded security applications.

Table 4. Secure Authenticator Evaluation Kits

Part Number	Evaluation Kit
DS28E38	DS28E38EVKIT
DS28C36	DS28C36EVKIT
DS2476	See Note 1
DS28E35	DS28E35EVKIT
DS2475	
MAX66242	MAX66300-24XEVKIT
MAX66240	
MAX66300	
DS28C22	DS28C22EVKIT

Part Number	Evaluation Kit
DS28E15	DS28E15EVKIT
DS28E22	DS28E22EVKIT
DS28E25	DS28E25EVKIT
DS2465	See Note 2
DS28EL15	DS28EL15EVKIT
DS28EL22	DS28EL22EVKIT
DS28EL25	DS28EL25EVKIT
DS24L65	See Note 2

Note 1: The DS2476 is included in the evaluation kits for DS28C36 and DS28E38.

Note 2: The DS2465 and DS24L65 are included in the evaluation kits for DS28E15/DS28C22/DS28E25 and DS28EL15/DS28EL22/DS28EL25.

Table 5. DeepCover Secure Microcontrollers for Embedded Security Applications

Part Number	Core	Frequency	Key Storage	USB	I²C	SPI	Symmetric Crypto	Asymmetric Crypto	Hash Algorithms
MAXQ1061	Built-in Firmware		Tamper-proof EEPROM		▪	▪	AES 128, 256	ECDSA P-256, P-384, P-521 ECDH	SHA-256, SHA-384, SHA-512
MAX32555	Cortex® M3	60MHz	Active tamper reaction	▪	▪	▪	AES 128, 192, 256 3DES	RSA 1024, 2048 ECDSA P-256, P-384, P-521 ECDH	SHA-224, SHA-256, SHA-384, SHA-512
MAXQ1050	MAXQ30	20MHz	Active tamper reaction	▪		▪	AES 128, 192, 256	RSA 1024, 2048 ECDSA P-192, P-256	SHA-224, SHA-256

MAXQ1061: DeepCover Secure Cryptographic Controller

The MAXQ1061 protects the confidentiality, authenticity and integrity of software IP, communication and revenue models.

It is ideal for IoT nodes, 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.

It handles encryption, ECDSA digital signature computation, and verification. It can also serve as a secure bootloader for an external generic microcontroller.

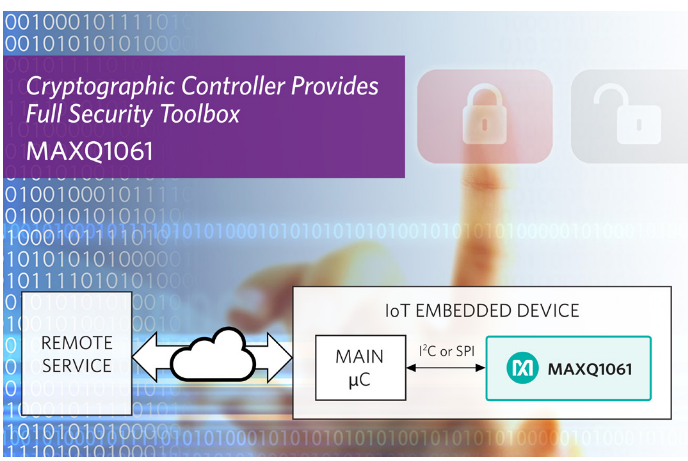

Figure 4. MAXQ1061

Key Features:

- Advanced Cryptographic Tool Box Seamlessly Supports Highly Secure Key Storage
- Make Certificates Distribution Easy
- High-Level Functions Simplify SSL/TLS/DTLS Implementations
- Multiple Communication Interface Options for Simpler Connection to a Host Processor
- Comprehensive Host Software Libraries are Provided
- Extensive Host/System Services Increase Flexibility and Reduce System Cost
- Fast AES Engine for Bulk Encryption
- No Firmware Development Required

DeepCover Secure Microcontrollers for Financial Transactions

Consumer payment habits are changing: chip cards are replacing magnetic stripe cards, contactless payment is now supported either by smartcards or smartphones, mobile POS terminals enable card acceptance for small merchants or home services, and countertop POS systems are adopting the tablet form factor. In the meantime, standards and payment schemes require even greater security. Supporting the increased flexibility expected by consumers, while at the same time guaranteeing the security of transactions, has become a permanent challenge for financial transaction systems designers. Maxim's expertise in this field has enabled the development of a wide range of secure microcontrollers supporting these trends.

For example, the **MAX32560** secure microcontroller (Figure 5) integrates an EMV-compliant integrated contactless reader interface that makes this device the first secure microcontroller to support PCI-PTS security and contactless payments.

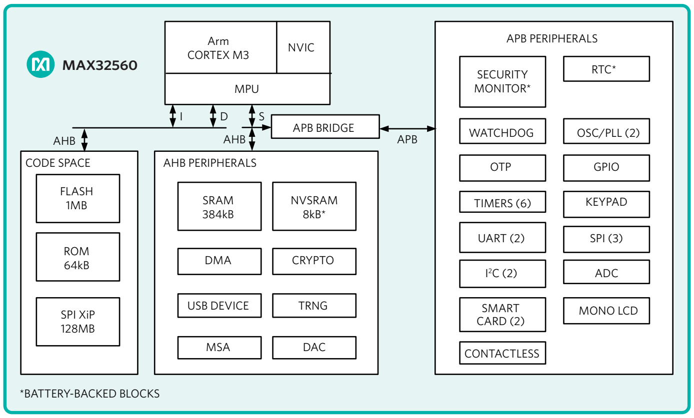

Figure 5. MAX32560 Block Diagram

Our secure microcontrollers feature:

- Active tamper reaction
- Hardware crypto accelerators
- Dedicated integrated analog interfaces for financial transactions
  - EMV-compliant smartcard PHY
  - Magnetic stripe card reader
  - EMV contactless
- Internal security monitors
- Advanced sensors for external tamper detection

Our expertise also goes beyond silicon. In addition to delivering secure microcontrollers with the latest security features, we also provide:

- EMV software stacks
- PCI-PTS evaluation reports
- Crypto libraries
- Full Linux BSP and PCI-PTS-compliant Linux code for **MAX32590**
- Support for PCI-PTS and EMV certifications

Secure Arm-Based Microcontrollers

Our Arm®-based secure microcontrollers (Figure 6) were designed to be used either as main processors or coprocessors for POS or mobile POS systems, pin pads or encrypted pin pads.

While these products offer a wide variety of tools, libraries and operating systems, they also provide advanced security features compliant with the latest standards. This unique combination accelerates time to market and leads to first-pass certification success. Table 6 lists DeepCover secure microcontrollers that support financial transaction applications.

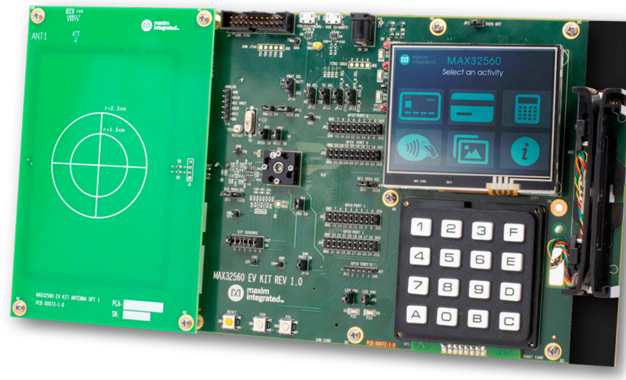

Figure 6. MAX32560 Evaluation Kit

Secure Microcontrollers for Magnetic Heads

The PIN Transaction Security (PCI-PTS) standard demands increasing levels of cardholder data protection, requiring magnetic card data to be highly protected in financial terminals. For this reason, we have designed microcontrollers (Figure 7) that can read and decode 3 tracks of magnetic stripe data and encrypt them before they are transmitted to the application processor, saving the implementation of costly physical protections. Table 7 and Figure 8 depict secure microcontrollers designed for magnetic head applications.

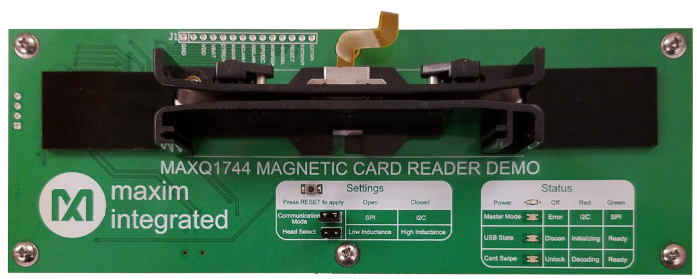

Figure 7. MAXQ1744 Evaluation Board

Secure Microcontroller Tool Sets

Our secure microcontroller development boards embed a comprehensive set of interfaces. They feature the most common payment-dedicated interfaces such as smartcard connectors, magnetic stripe heads, keyboards and displays.

Our Arm-based secure microcontroller development tools are based on popular open-source IDE, compilers, and debuggers. By leveraging the Arm core they reduce development times and accelerate time to market.

Table 6. DeepCover Secure Microcontrollers for Financial Transaction Applications

	MAX32590	MAX32550	MAX32552	MAX32560	MAX32555
Core	Arm 926EJ-S	Cortex-M3	Cortex-M3	Cortex-M3	Cortex-M3
Flash/SRAM	—/384KB	1MB/256KB	1MB/384KB	1MB/384KB	512KB/96KB
Contactless Interface	—	—	—	Yes	—
TFT Controller/Mono LCD	Yes/Yes	Yes/Yes	No/Yes	No/Yes	No/Yes
Clock Speed	384MHz	108MHz	108MHz	108MHz	60MHz
AES Encrypted NVSRAM	24KB	8KB	8KB	8KB	1KB
Dynamic Sensor Pairs	6	6	6	6	4
OTP	2KB	4KB	4KB	4KB	4KB
MSR Decoder/Smartcard UART/Smartcard PHY	—/2/—	1/1/1	1/2/1	1/2/2	1/1/2
ADC	3-channel 10-bit	2-channel 10-bit	2-channel 10-bit	2-channel 10-bit	6-channel 10-bit
DAC	—	1-channel 8-bit	1-channel 8-bit	1-channel 8-bit	1-channel 8-bit
USB Device/SPI/UART/I²C	1/5/3/1	1/3/2/1	1/3/2/1	1/3/2/1	1/3/3/1
Ethernet MAC	Yes	—	—	—	—
USB Host	1	—	—	—	—
External Memories	NAND/NOR Flash Encrypted LPDDR	—	Quad SPI with XiP	Quad SPI with XiP	—
Timers	3	6	6	6	8
GPIO	160	70	69	69	70
Package	BGA324	BGA121	BGA121	BGA144	BGA121

Table 7. DeepCover Secure Microcontrollers for Magnetic Head Applications

<table>
<tr><th></th><th>Core/Frequency</th><th>Memories</th><th>Interfaces</th><th>Crypto</th><th>Others</th></tr>
<tr><td>MAXQ1741</td><td>MAXQ20 at 12MHz</td><td>16kB Flash
1kB SRAM</td><td>1 UART
2 SPI
1 I²C</td><td>AES</td><td>—</td></tr>
<tr><td>MAXQ1743</td><td colspan="2" rowspan="2">Turnkey embedded firmware provided by Maxim</td><td rowspan="2">1 I²C
1 SPI</td><td rowspan="2">AES, 3DES</td><td>—</td></tr>
<tr><td>MAXQ1744</td><td>Ultra-low power:
450µA during card reading</td></tr>
</table>

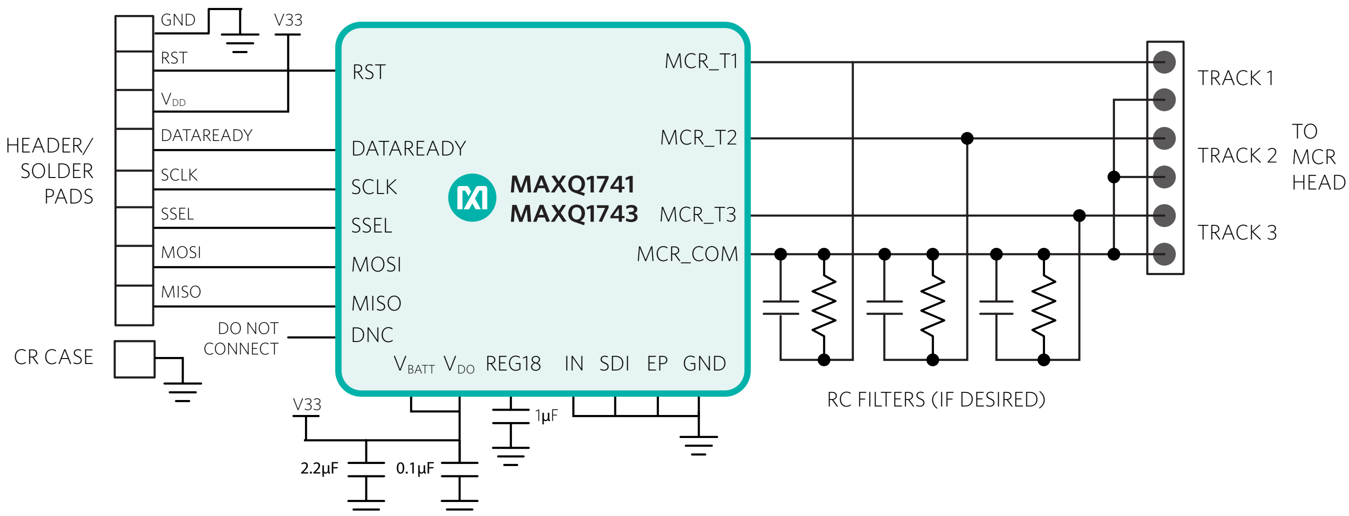

Figure 8. MAXQ1741/MAXQ1743

Trademarks

DeepCover and 1-Wire are registered trademarks and ChipDNA is a trademark of Maxim Integrated Products, Inc.
Arm and Cortex are registered trademarks and registered service marks, and Mbed is a trademark of Arm Limited.
MicroZed and ZedBoard are trademarks of Avnet, Inc.
Xilinx, Zynq, and Spartan are registered trademarks and Xilinx is a service mark of Xilinx, Inc.

Learn more

For more information, visit:
www.maximintegrated.com/DeepCover

November 2017; Rev. 4