Protect It All with DeepCover Embedded Security Solutions

Security requirements are getting tougher. Hackers are more sophisticated, and the stakes are higher than ever. You need multiple layers of security to protect your embedded systems. But without a dedicated team of security experts behind you, adding the right protection to your system can be challenging.

Our DeepCover® product line gives you the benefit of our security expertise, enabling you to quickly integrate advanced physical security to achieve the highest level of protection possible. DeepCover embedded solutions comprise three families of products with the most up-to-date physical security to meet all your application needs.

- **DeepCover Secure Microcontrollers** integrate advanced cryptography and physical security to offer the highest level of protection against physical tampering and reverse engineering.
- **DeepCover Secure Authenticators** implement advanced physical security to provide the ultimate in low-cost IP protection, clone prevention, and peripheral authentication.
- **DeepCover Security Managers** combine advanced physical security with on-chip, nonimprinting memory to safeguard sensitive data from the slightest physical or environmental tampering.

When you need it secure, we’ve got you covered.
Advanced Protection, Deepest Security

Security is a must, and no system-on-chip (SoC) µC delivers protection like Maxim Integrated’s DeepCover® Secure Microcontrollers. Our devices integrate advanced cryptography and physical security to offer the highest level of protection against physical tampering and reverse engineering.

Go Meshless

Secure SoC with On-the-Fly Memory Encryption

The DeepCover Secure Microcontroller (MAX32590 (JIBE)) is a secure, ARM9™-based, SoC µC with a 384MHz clock speed and Ethernet interface communication to meet stringent financial terminal requirements. Our patented on-the-fly encryption technology keeps your code safe without the hassle of expensive mesh. PCI PTS 3.1 certification is easy with an extensive board support package and Linux® OS support, innovative security mechanisms, and high integration. Replace the traditional mono LCD with a colorful TFT display to provide better visual effects for your designs.

Features

- Extensive security mechanisms (authenticated boot, secure NV SRAM with instant erase, OTP, AES/SHA engines, dynamic sensor controller, temperature/voltage and frequency monitors, secure package)
- High system integration (Ethernet, TFT LCD, 384MHz CPU, USB host and device)
- Real-time external memory encryption and integrity

Benefits

- Reduced BOM with fewer external communication controllers; better user experience with color TFT display
- Provides best confidentiality while removing the need for an additional security cover; prevents code injection
- Simplifies security architecture and eases PCI certification
Your PCI PTS 3.1 Terminal...Now

**JIBEPOS PCI PTS-Ready Reference Design Reduces Time to Market**

Build your financial terminal with confidence that it will pass PCI evaluation.

Powered by the DeepCover Secure Microcontroller (MAX32590), the JIBEPOS reference design provides the fastest route to getting your terminal certified. Start with our meshless design, patented secure keypad layout, BOM-optimized hardware, SPA/DPA-resistant cryptographic library, certified EMV® L1 library, PCI PTS-compliant secure Linux OS, and a security handbook to adapt the design to your own enclosure.

- 3.5in TFT color display
- Haptic resistive touch screen
- Secure magnetic card reader
- Ethernet 10/100, V90 modem, USB
- NFC contactless reader
- Thermal printer
- On-board audio

Protect Magnetic Strip Data at the Source

**End-to-End Encryption Made Easy**

The DeepCover Secure Microcontroller (MAXQ1741) provides a high level of security for the magnetic stripe reader (MSR) by placing an ultra-secure µC with high-speed hardware encryption inside the magnetic card reader head. Rather than transmitting sensitive data in cleartext, the MAXQ1741 automatically encrypts the data at the swipe. Furthermore, the device provides a convenient, secure, nonvolatile storage space for storing various security keys that is protected against physical tampering.
One-Chip PIN Pad Solution

The DeepCover Secure Microcontroller (MAXQ1852*) features a single-cycle 16-/32-bit RISC processor and hardware-accelerated symmetric and asymmetric encryption engines, as well as extensive communication interfaces including ISO 7816, USB, and SPI. It has the flexibility to be a stand-alone controller for any PCI-PTS 3.1 PIN pad application or a coprocessor for financial terminals or any other secure applications. System cost is optimized with extensive GPIO pins to drive a keypad and LCD display, large system SRAM, and integrated dynamic tamper sensors. These dynamic sensors are fed by a true random signal that prevents from any bypass attempt. Furthermore upon tampering, the internal AES-256 master key that is used to encrypt the contents of the battery-backed SRAM is instantly erased. The device also makes product manufacturing and field upgrades much simpler by offering a public key (ECDSA)-based secure bootloader for programming the internal flash.

Security Features

- Hardware crypto engines for AES, 3DES, RSA, DSA, ECDSA, SHA-1, SHA-224, and SHA-256
- True random-number generator (TRNG)
- Multiple dynamic sensor inputs and environmental sensors
- 4KB AES encryptable NV SRAM with instant master key zeroization upon tampering
- Built-in voltage regulator for single power-supply operation
- ECDSA bootloader

High-Performance µC

- 16-/32-bit, single-cycle RISC core
- Internal 256KB of flash memory
- 8KB of system SRAM
- USB interface, ISO 7816 controller, RTC, USART, and SPI bus
- 68-pin TQFN or 64-ball CSBGA package

*Future product—contact the factory for availability.
Stop Counterfeiters from Stealing Your IP

Your R&D is very valuable, so protect it from counterfeiters who want to produce and sell it. Our DeepCover® Secure Authenticators implement advanced physical security to provide the ultimate in low-cost IP protection, clone prevention, and peripheral authentication. Options range from secure, crypto-strong, FIPS 180-based challenge-and-response bidirectional authentication to customization of unalterable 64-bit, factory-programmed serial numbers.

- OEM authentication
- System copy protection
- HW/SW license management
- Tamper-proof feature settings
- Safety/quality assurance

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
<th>Host Interface</th>
<th>Authentication Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS2465</td>
<td>SHA-256 coprocessor with 1-Wire® Master</td>
<td>I2C</td>
<td>Secure storage of system secret</td>
</tr>
<tr>
<td>DS28E15, DS28E22, DS28E25</td>
<td>SHA-256 with 0.5Kb/2Kb/4Kb EEPROM</td>
<td>1-Wire</td>
<td>Bidirectional challenge and response</td>
</tr>
<tr>
<td>DS28CN01</td>
<td>SHA-1 with 1Kb EEPROM</td>
<td>I2C/SMBus</td>
<td>Bidirectional challenge and response</td>
</tr>
<tr>
<td>DS28E01-100, DS28E02</td>
<td>SHA-1 with 1Kb EEPROM</td>
<td>1-Wire</td>
<td>Bidirectional challenge and response</td>
</tr>
<tr>
<td>DS28E10</td>
<td>SHA-1 with 224b OTP EPROM</td>
<td>1-Wire</td>
<td>Challenge and response</td>
</tr>
<tr>
<td>DS2460</td>
<td>SHA-1 coprocessor</td>
<td>I2C</td>
<td>Secure storage of system secret</td>
</tr>
<tr>
<td>MAX66040, MAX66140</td>
<td>SHA-1 with 1Kb EEPROM</td>
<td>RF</td>
<td>Bidirectional challenge and response, ISO 14443B/15693</td>
</tr>
<tr>
<td>DS2431</td>
<td>1Kb EEPROM</td>
<td>1-Wire</td>
<td>Customized 64-bit ROM, WP/OTP modes</td>
</tr>
<tr>
<td>DS2401, DS2411</td>
<td>64-bit ROM serial number</td>
<td>1-Wire</td>
<td>Customized 64-bit ROM</td>
</tr>
</tbody>
</table>

Newest SHA-256 Products Solve Host and Slave Device Needs

- SHA-256 HW co-processing to operate connected slave devices
- Highly secure storage of system solution secret
- 1-Wire line driving for slave device I/O
- Low-power mode: 500nA (typ) at 3.3V

Contact the factory for 1.8V options.
Easily Add System Security

DeepCover Security Managers Provide Total Hardware Security with No System Redesign

Maxim Integrated’s extensive DeepCover® Security Managers allow users to add advanced physical security to systems using their existing system microprocessor. The ICs have a proprietary “nonimprinting” memory that stores critical data, but immediately and completely erases this memory upon qualified tamper events. The security managers also provide continuous tamper detection, regardless of the power source.

- Work with your existing microprocessor
  - I2C or SPI interfaces available
- Internal secure memory
  - Nonimprinting memory
  - Densities from 64B to 4KB
- Internal tamper monitors
  - Temperature, including rate of change
  - Power
  - Oscillator
- Monitor external circuitry for tampers
- Real-time clock/counter
  - Tamper-event timestamping
- Small CSBGA footprint and package
- Low power consumption during battery backup
- Monitor main power
  - Automatically switch from main power to battery
- Provide power and erase an external SRAM

Hardware AES Encryption with Anti-Tamper and Nonimprinting Memory Provides Industry’s Highest Level of Security

The DeepCover Security Manager (MAX36025) provides hardware encryption and the most advanced anti-tamper features offered in the market. Encrypting/decrypting data in hardware using the MAX36025 provides the highest level of security, as opposed to software encryption on a general-purpose microcontroller. The keys never leave the MAX36025 and are kept more secure with the tamper-detection features.

General Features
- Dual AES processors
  - Supports 128-, 192-, and 256-bit keys
  - ECB, CTR, and CBC modes
- Authentication via an encrypted I2C interface
- Bidirectional SPI ports
  - Use the same key to encrypt/decrypt data
  - Support for independent encryption/decryption streams

Security Features
- 1KB nonimprinting memory for encryption key storage
- Segmented memory to store two sets of critical data
- Temperature, power, and oscillator tamper monitors
- Digital and analog input tamper monitoring

No code needed to communicate with MAX36025 AES engine after authentication

No resident software development required

![Diagram of the DeepCover Security Manager (MAX36025)]
## Secure Microcontrollers

<table>
<thead>
<tr>
<th>Part</th>
<th>Speed and Core</th>
<th>Internal Flash/SRAM Memory (KB)</th>
<th>Secure NV SRAM (KB)</th>
<th>External Memory</th>
<th>USB</th>
<th>SPI</th>
<th>ISO 7816</th>
<th>GPIO</th>
<th>Battery Leakage (µA)</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAXQ1004</td>
<td>6MHz, MAXQ20</td>
<td>16/640B</td>
<td></td>
<td>—</td>
<td>—</td>
<td>1</td>
<td>—</td>
<td>8</td>
<td>300nA</td>
<td>16-TQFN</td>
</tr>
<tr>
<td>MAXQ1010</td>
<td>12MHz, MAXQ20</td>
<td>128/2</td>
<td>1288</td>
<td>—</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>31</td>
<td>400nA</td>
<td>48-TQFN</td>
</tr>
<tr>
<td>MAXQ1011*,</td>
<td>12MHz, MAXQ20</td>
<td>64, 32/1</td>
<td>1288</td>
<td>—</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>31</td>
<td>400nA</td>
<td>48-TQFN</td>
</tr>
<tr>
<td>MAXQ1050</td>
<td>25MHz, MAXQ20</td>
<td>128/12</td>
<td>256B + 4KB AES encryptable</td>
<td>—</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>20</td>
<td>240nA</td>
<td>40-TQFN</td>
</tr>
<tr>
<td>MAXQ1740,</td>
<td>12MHz, MAXQ20</td>
<td>16/—</td>
<td>1152B</td>
<td>—</td>
<td>—</td>
<td>2</td>
<td>—</td>
<td>16</td>
<td>3</td>
<td>28-TQFN</td>
</tr>
<tr>
<td>MAXQ1850</td>
<td>16MHz, MAXQ30</td>
<td>256/—</td>
<td>8</td>
<td>—</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>16</td>
<td>130nA</td>
<td>40-TQFN, 49-CSBGA</td>
</tr>
<tr>
<td>MAXQ1851*</td>
<td>16MHz, MAXQ30</td>
<td>256/8</td>
<td>256-bit + 4KB AES encryptable</td>
<td>—</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>16</td>
<td>350nA</td>
<td>40-TQFN, 49-CSBGA</td>
</tr>
<tr>
<td>MAXQ1852*</td>
<td>16MHz, MAXQ30</td>
<td>256/8</td>
<td>256-bit + 4KB AES encryptable</td>
<td>—</td>
<td>D</td>
<td>1</td>
<td>1</td>
<td>32</td>
<td>350nA</td>
<td>40-TQFN, 49-CSBGA</td>
</tr>
<tr>
<td>USIP</td>
<td>96MHz, MIPS32*</td>
<td>4KSd™</td>
<td>256/128</td>
<td>512-bit</td>
<td>O</td>
<td>1</td>
<td>3</td>
<td>2.9</td>
<td>256-512-bit</td>
<td>256-CSBGA</td>
</tr>
<tr>
<td>ZA9L0</td>
<td>180MHz, ARM922T</td>
<td>—/64</td>
<td>4</td>
<td>NOR flash, SRAM, SDRAM</td>
<td>—</td>
<td>1</td>
<td>2</td>
<td>21</td>
<td>256-512-bit</td>
<td>256-CSBGA</td>
</tr>
<tr>
<td>MAX32580*</td>
<td>192MHz, ARM926EJ-S</td>
<td>—/384</td>
<td>256-bit + 24KB AES encryptable</td>
<td>—</td>
<td>D</td>
<td>2</td>
<td>6</td>
<td>129</td>
<td>256-512-bit</td>
<td>169-CSBGA</td>
</tr>
<tr>
<td>MAX32590</td>
<td>384MHz, ARM926EJ-S</td>
<td>—/384</td>
<td>256-bit + 24KB AES encryptable</td>
<td>NOR flash, NAND SRAM, SDRAM LPDDR</td>
<td>D, H</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>256-512-bit</td>
<td>324-CSBGA</td>
</tr>
</tbody>
</table>

D = device port, O = OTG port, H = host port

## Security Managers

<table>
<thead>
<tr>
<th>Part</th>
<th>Temp Range (°C)</th>
<th>Power Consumption (typ) (µA)</th>
<th>Nonimprinting Memory (KB)</th>
<th>External Tamper Monitors</th>
<th>I/O</th>
<th>Authentication</th>
<th>AES Encryption ECB/CTR/CBC Modes</th>
<th>EV Kit</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS3600,</td>
<td>-40 to +85</td>
<td>5.7</td>
<td>64B (DS3600)</td>
<td>4</td>
<td>3-wire/1°C</td>
<td>—</td>
<td>Encrypted 1°C 2 AES engines</td>
<td>✓</td>
<td>25-CSBGA</td>
</tr>
<tr>
<td>DS3605</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS3640,</td>
<td>-40 to +85</td>
<td>6.5</td>
<td>1</td>
<td>4</td>
<td>4-wire/1°C</td>
<td>—</td>
<td></td>
<td>✓</td>
<td>25-CSBGA</td>
</tr>
<tr>
<td>DS3641</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS3645</td>
<td>-55 to +95</td>
<td>12</td>
<td>4</td>
<td>8</td>
<td>1°C</td>
<td>—</td>
<td></td>
<td>✓</td>
<td>49-CSBGA</td>
</tr>
<tr>
<td>DS3650,</td>
<td>-40 to +85</td>
<td>3.0, 1.5</td>
<td>128B</td>
<td>2</td>
<td>4-wire</td>
<td>—</td>
<td></td>
<td>✓ (MAX36051)</td>
<td>16-CSBGA</td>
</tr>
<tr>
<td>MAX36051</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX36025</td>
<td>-55 to +95</td>
<td>9</td>
<td>1</td>
<td>8</td>
<td>SPI (2)</td>
<td>Encrypted 1°C 2 AES engines</td>
<td>✓</td>
<td>81-CSBGA</td>
<td></td>
</tr>
</tbody>
</table>

*Future product—contact factory for availability.

DeepCover and 1-Wire are registered trademarks of Maxim Integrated Products, Inc.
ARM9 and ARM926EJ-S are trademarks of ARM Limited.
EMV is a registered trademark of EMVCo LLC.
Linux is a registered trademark of Linus Torvalds.
MIPS32 is a registered trademark and 4KSd is a trademark of MIPS Technologies, Inc.

Contact Maxim Direct at 1.888.629.4642 or for more information, visit www.maximintegrated.com.

© 2013 Maxim Integrated Products, Inc. All rights reserved. Maxim integrated and the Maxim Integrated logo are trademarks of Maxim Integrated Products, Inc., in the United States and other jurisdictions throughout the world. All other company names may be trade names or trademarks of their respective owners.

Rev 2; May 2013