



Maxim > Design Support > Technical Documents > Application Notes > Embedded Security > APP 4244

Maxim > Design Support > Technical Documents > Application Notes > Memory > APP 4244

Keywords: POS, PIN pads, FIPS-140.2, common criteria, PCI-PED, EMV-4.1

APPLICATION NOTE 4244

Secure Managers Provide Multifaceted Monitoring to Ensure System Security

Jun 18, 2008

Abstract: This article describes many of the embedded security features in the various DS36xx secure manager products.

Introduction

Intrusion prevention in many systems had traditionally been left to the specific demands of that application and to the individual creativity of the system designer. To provide enhanced security in an ever-more-interconnected society, various entities have defined specific standards to eliminate potential holes in the creation of a "secure system." Whether the system is a cash register or a file server, the task of security is essentially identical: prevent any open path for a hacker trying to compromise that system security.

Secure Managers

The DS36xx secure manager products integrate a CPU supervisor, NVSRAM controller, real-time clock (RTC), temperature sensor, analog-to-digital converter (ADC), random number generator (RNG), and the I/Os and support circuitry necessary to operate this monitoring device on either system power or a battery. These products reduce component count and unload the continuous system monitoring requirements that would otherwise be placed on the processor in secure applications such as point-of-sale (PoS) terminals, PIN pads, secure communications, set-top boxes, alarm systems, or gaming systems. The secure manager products support the highest security level requirements of the FIPS-140.2, Common Criteria, PCI-PED, and EMV-4.1 certification entities. **Table 1** presents selection options presently available or in development.

Table 1. Secure Manager Product Selection Guide

Part Number	I/O	Analog Voltages Monitored ¹	Digital Inputs Monitored	Internal Key Memory	External Memory Control	Random Number Generator	Over-Voltage Monitor	Battery Monitor
DS3600	3-wire	4	1	64B	✓	✓		✓
DS3605	I ² C	4	1	—	✓	✓		✓
DS3640	I ² C	5	3	1024B		✓	✓	✓
DS3641	4-wire	5	3	1024B		✓	✓	✓
DS3645	I ² C	12	4	4096B	✓	✓	✓	✓
DS3650	4-wire	2	—	—			✓	✓
DS3655	I ² C	—	4	64B				

¹Does not include V_{CCI} and V_{BAT} monitors.

The secure manager products are low-cost, space-efficient components that offer a premier security solution for many applications. By using the high levels of integration in these devices, valuable system resources can be fully utilized for the principal application while the secure manager handles the generally mundane, but very critical, security monitoring chores.

Tamper Response

All tamper inputs are constantly monitored in parallel. At the instant in which any tampering is detected, the following simultaneous actions are initiated:

1. Tamper latches record the monitor channel that initiated the tamper event
2. The tamper output asserts to alert the system processor
3. The current time is frozen in the Time Stamp registers
4. Encryption key memory is immediately erased (if applicable)
5. External SRAM memory is immediately erased (if applicable)

Recovery from a tamper event begins with identification of the source of the event. The tamper latches and the event time stamp will remain frozen until the condition causing the tamper event has been corrected and the latches have been reset.

Power-Supply Monitoring

A traditional CPU supervisor function monitors the V_{CCI} power supply, providing a reset signal to the microprocessor when the supply is out of tolerance. A tamper reaction to an abnormally high V_{CCI} supply is also included in many of the products.

Battery-Supply Monitoring

An ADC register monitors the battery voltage, which is readable through the I/O port. Tamper reaction to an abnormally low or high battery voltage is included in most of the product offerings.

Time Keeping and Tamper-Event Time Stamp

The integrated RTC provides a time reference for tamper-event recording and recovery. Time-of-day alarm and CPU watchdog functions are also included in many of the product offerings.

External Analog Supply Monitoring

Besides the internal V_{CC1} and V_{BAT} monitoring functions, the secure manager products offer multiple configurations of analog inputs. These inputs monitor external power supplies or other critical bias conditions, depending on specific application requirements.

External Digital Signal Monitoring

Most of these devices also include digital input channel(s), which can be utilized for a tamper response to some user-defined conditions. Using standard TTL input thresholds, these inputs could be directly fed from other on-board logic controls. If needed, the inputs can be configured with a resistive-divider network to monitor additional bias sources.

Internal Encryption Key Memory

Most of the devices include a nonvolatile encryption key memory array, accessible through the I/O port. In the event of a tamper, the encryption key memory is rapidly erased.

External Memory Control and Security

Several of the secure manager products include a tamper-reactive nonvolatile SRAM controller, with provisions to supply battery-backed power and control logic for external memory support. When V_{CC1} power is within tolerance, the external SRAM is powered from that V_{CC1} supply. Should the external power supply fail, access to the SRAM is inhibited. The battery is automatically switched in to provide backup power to that external memory.

Power for External Support Circuitry

A battery-backed power supply output is provided for any critical external support circuitry required for continuous operation. The output supply voltage is either the V_{CC1} supply, if within the defined tolerance, or V_{BAT} .

Random Number Generator

Most of the secure manager products contain a pseudo-random number generator (RNG), which provides a seed value for the user to generate their own FIPS 140.2-compliant random number. Upon initial application of V_{CC1} power, the RNG is seeded using several natural sources of randomness. Until the device is ready, the RNG will output zeros data. Once a non-zero byte is read, any number of additional random bytes can be read in 128-byte blocks. This read cycle can be repeated any number of times until the user has retrieved sufficient random data to seed a software-controlled random number generation.

Thermal Monitoring

An on-chip temperature sensor monitors the system environment. High- and low-temperature limits, and

appropriate tamper reaction if those operational limits are violated, counter any intended thermal attack.

Discrete System Identification

Each device contains a unique serial number, readable through the I/O port. This silicon serialization allows for discrete end-item system identification. The products are manufactured so that no two devices will ever contain the same serial number.

BGA Packaging

The product family is offered in chip-scale ball grid array (CSBGA) packages. By minimizing exposed pins, this packaging further enhances the security of the data and control signals.

Related Parts		
DS3600	DeepCover Security Manager with 64B Nonimprinting, Battery-Backed Encryption Key SRAM	Free Samples
DS3605	DeepCover Security Manager for NV SRAM Control with RTC and Thermal Tamper Detection	Free Samples
DS3640	DeepCover Security Manager with I ² C Interface and 1KB Nonimprinting Battery-Backed Encryption Key SRAM	Free Samples
DS3641	DeepCover Security Manager with SPI-Compatible Interface and 1KB Nonimprinting Key Memory	Free Samples
DS3644	DeepCover Security Manager with 1KB Secure Memory and Programmable Tamper Hierarchy	Free Samples
DS3645	DeepCover Security Manager with 4KB Secure Memory and Tamper Protection	Free Samples
DS3650	DeepCover Security Manager with Thermal Tamper Detection	Free Samples
DS3655	DeepCover Security Manager with Ultra-Low-Power Tamper Detection and Nonimprinting Memory	Free Samples
DS3660	DeepCover Security Manager for Low-Voltage Operation with 1KB Secure Memory and Programmable Tamper Hierarchy	
MAX36025	DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption	
MAX36051	DeepCover Security Manager with 128 Bytes of Nonimprinting Memory	

More Information

For Technical Support: <http://www.maximintegrated.com/support>

For Samples: <http://www.maximintegrated.com/samples>

Other Questions and Comments: <http://www.maximintegrated.com/contact>

Application Note 4244: <http://www.maximintegrated.com/an4244>

APPLICATION NOTE 4244, AN4244, AN 4244, APP4244, Appnote4244, Appnote 4244

© 2013 Maxim Integrated Products, Inc.

Additional Legal Notices: <http://www.maximintegrated.com/legal>