Keywords: Secure Supervisor, Secure Controller, Secure memory, secure SRAM, Secure SRAM controller, Battery backed controller, POS, ATM, SDR, Software Defined Radio, communication, secure communications, FIPS, FIPS140.2, encryption keys, data protection

APPLICATION NOTE 4185

Addressing the Physical Security of Encryption Keys

Feb 21, 2008

Abstract: Physical security of an encryption key, especially in portable applications such as secure radios, is of prime consideration in military applications. However, it is possible to achieve compliance with applicable regulations, as well as provide additional layers of protection, using specially designed components. These components use electrical and physical design techniques for the secure generation and storage of digital encryption keys.

This article was also featured in Maxim's Engineering Journal, vol. 62 (PDF, 1.3MB).

The essence of secure communications is protecting the encryption key. While large encryption keys can provide a certain degree of protection against brute-force computational techniques to break a code, this protection does not address the need for physical security, which is equally important. To properly address physical security, several issues must be considered. These include: a physical mechanism for generating random keys, a physical design that prevents covert electronic interception of a key that is being communicated between authorized agents, and a secure method of storing a key that protects against clandestine physical and mechanical probing.

Using a host of features that range from package design, to external-sensor interfaces, to internal circuit architectures, Maxim's DS36xx family of secure supervisors provides all of these capabilities to military electronics design engineers. Devices with such features can simplify compliance with security requirements for both mature and emerging portable military computing and communications systems. The range of possible applications for these devices is, therefore, wide and diverse, as indicated in **Figure 1**.

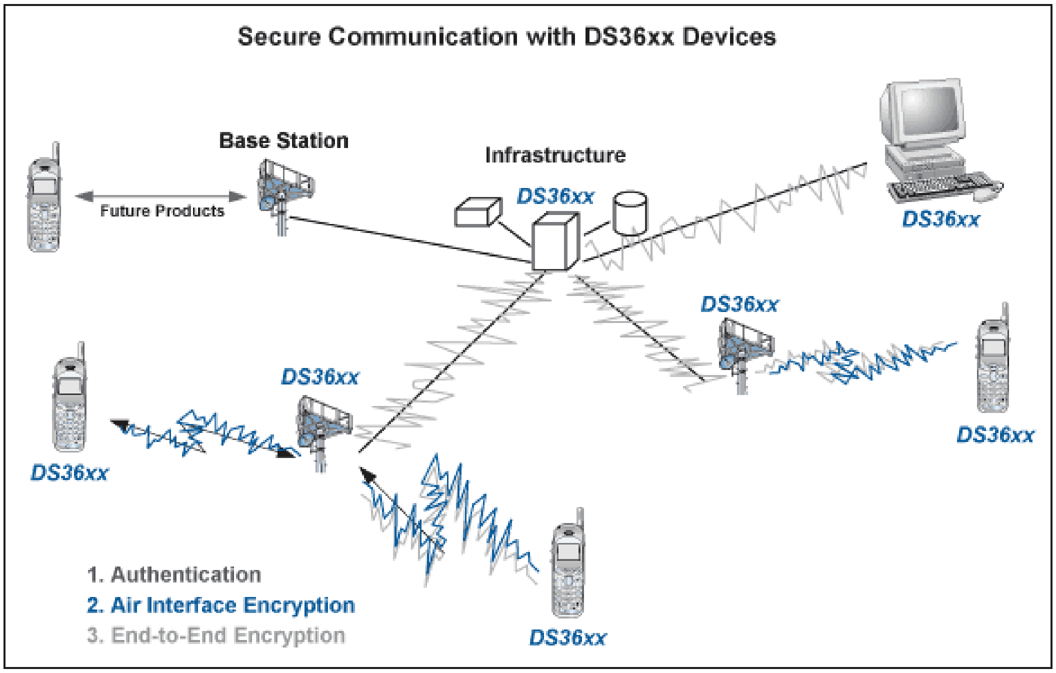

Figure 1. The DS36xx devices are suited for a wide range of present and future military and homeland security communications functions, including secure communications and client authentication.

Security Requirements for Electronic Data

The Federal Information Processing Standard (FIPS) is a standard that describes the U.S. government's requirements that cryptographic modules must meet for sensitive, but unclassified, uses. This standard is published by the National Institute of Standards and Technology (NIST). The FIPS 140-2 standard has four basic levels:

- Security Level 1: No Physical Security Mechanisms Required (Just Implements NIST Standardized Cryptographic Algorithms)
- Security Level 2: Tamper-Evident Physical Security
- Security Level 3: Tamper-Resistant Physical Security
- Security Level 4: Physical Security Provides an Envelope of Protection

For advanced-security military communication applications, designs must also meet National Security Agency (NSA) Type 1 certification standards. Equipment certified by the NSA is used to cryptographically secure classified U.S. government information. The certification process is rigorous and includes testing and analysis of the following items:

- Cryptographic Security
- Functional Security
- Tamper Resistance
- Emissions Security
- Security of Product Manufacturing and Distribution

A common example of an application that must comply with these guidelines is communications equipment designed to operate within the Warfighter Information Network-Tactical (WIN-T), which is the tactical communications protocol for warfighters. WIN-T supports a broad range of data, voice, and video capabilities. This network helps the warfighter stay connected at all times from any location by providing mobile, reliable, high-bandwidth communications. The capabilities provided by WIN-T are delivered by utilizing popular communications technologies, like a wireless local-area network (WLAN), voice-over-Internet protocol (VoIP), and third-generation cellular/satellite technology. WIN-T links warfighters located in tactical ground units with their commanders throughout the Department of Defense's (DoD's) worldwide network.

As with any military application, information security for WIN-T is extremely important. With WIN-T, the architecture must allow authorized users free access to the network, but also detect and deny unauthorized attacks. As such, WIN-T security must be built-in from the outset, rather than added on as an afterthought. This approach ensures safe and secure transmission of voice communications and digital data across the network.

In the past, systems were designed primarily for speedy deployment, often leaving security functions to be implemented as upgrades in the field. This happened because built-in security functions were usually considered to be quite expensive and a cause of schedule delays. However, all military communication applications now require a higher level of security from the outset to provide enhanced interoperability, connectivity, and regulatory compliance with FIPS 140-2, NSA, and WIN-T requirements. Security and intrusion prevention are increasingly crucial factors for other military applications as well. For example, General Dynamics®, together with Secure Computing®, recently developed the MESHnet Firewall for use in battlefield vehicles.

As a result, new military communications systems or components are no longer released without first meeting all of the applicable standards. Specifically, military communication applications are now required to meet, at a minimum, FIPS 140-2 Security Levels 3 and 4. Furthermore, in higher-level applications, the design engineer must adhere to NSA Type 1 and/or the newly implemented WIN-T requirements. Typically, at a minimum, military applications require a Security Level 3 certification for FIPS 140-2.

Achieving Compliance with Security Requirements

Addressing the security requirements set forth by the U.S. government is a complicated task for system designers. Security standards can (and should) change as often as the perceived threats for which they are developed, and generally become more stringent over time.

Keeping abreast of the ever-changing security standards can become troublesome for designers, because the design process must be guided by both the level of security required and the end purpose of the secure equipment to be designed. For example, security of an encryption key is not significantly increased by merely re-encrypting the keys, because sophisticated techniques have been developed to read encrypted keys. Therefore, keeping encryption keys secure from these techniques must be addressed using a combination of several different methods, including the enhancement of physical security.

When designing secure military systems that meet FIPS 140-2 (Security Levels 3 or 4), NSA Type 1, or WIN-T requirements, it is important to incorporate components that provide comprehensive tamper protection, even in the absence of main power. Members of Maxim's DS36xx family, such as the DS3600 shown in **Figure 2**, offer integrated solutions to secure both encryption keys and critical data by actively detecting tampers, even while on battery power (which engages immediately and transparently in the absence of main power). The on-chip power-supply monitor and battery switch ensure that all tamper-detection mechanisms remain active, regardless of the power source. Main power is constantly monitored—when it falls below the low threshold, an external backup battery is instantly and automatically switched in to keep both the internal and external protection circuitry alive. Thus, tamper detection is not interrupted with the loss of the equipment's main power source.

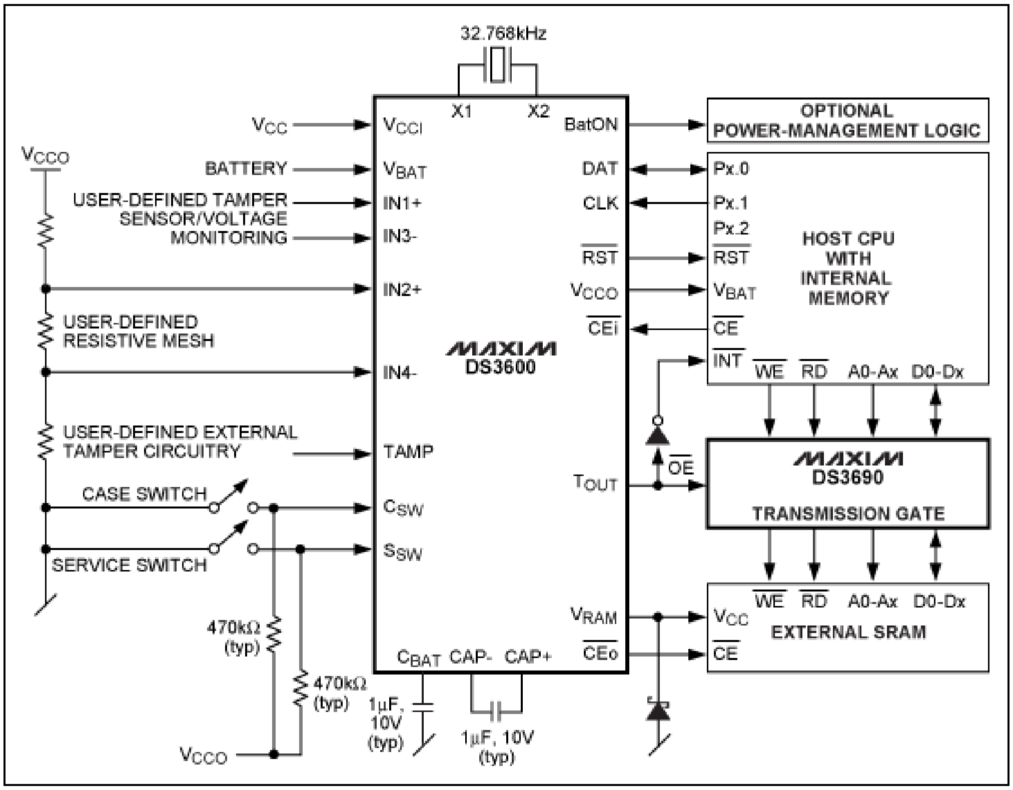

Figure 2. The DS3600 secure supervisor uses a combination of features and mechanisms to detect tampering and protect the contents of battery-backed volatile memory, such as internally stored encryption keys, or other sensitive data stored in an external SRAM.

To comply with the requirements of FIPS 140-2 (Security Levels 3 and 4), as well as the NSA Type 1 and WIN-T specifications, tamper detection components must allow the designer to attach their own external sensors, so that an envelope of protection—that is, a security boundary—can be provided around the devices storing the protected data. Attaching external sensors to the DS36xx series, the system designer has a unique and flexible method for adding layers of security to the application, thereby meeting many of the applicable requirements set forth by governing agencies.

To meet these various governmental requirements, analog supply voltages, digital signals, and a resistive-mesh protective sensor grid can all be easily and simultaneously monitored by the DS36xx secure supervisors. Furthermore, all DS36xx devices are offered in chip-scale ball-grid-array (CSBGA) packages (see **Figure 3**). By severely restricting access to the pins of a mounted device, these packages provide yet another layer of passive physical security for the control and data signals.

Figure 3. The CSBGA package of the DS36xx family provides a layer of passive protection by limiting access to I/O signals when the device is installed on a circuit board.

Internal Security Features

The DS36xx devices also include additional layers of protection in the form of internal tamper-detection mechanisms. These internal mechanisms compliment the device's ability to interface to a customized configuration of external tamper-detection sensors. The internal tamper-detection mechanisms, which include an on-chip temperature sensor, case-switch monitor, power-supply monitor, battery monitor, and oscillator monitor, provide continuous tamper-detection monitoring. This monitoring remains active at all times, especially when running on battery power.

As with the external mechanisms, the internal mechanisms are triggered when user-defined and/or factory-programmed thresholds are violated. For example, in order to meet the prerequisites of certification bodies, such as the NSA, and those governing the FIPS and WIN-T standards, the designer can use the internal temperature sensor, which monitors the substrate temperature. Once either the upper or lower temperature limits are violated, a tamper response is initiated by the device.

Besides measuring instantaneous temperature, an additional temperature-monitoring function is provided by the DS36xx devices. Specifically, a rate-of-change detector monitors the speed at which the substrate temperature changes. A rapid increase or decrease in temperature triggers a tamper response in the device, which provides additional protection against advanced, clandestine data-recovery techniques.

One documented method of recovering data from protected SRAM involves the application of liquid nitrogen prior to the removal of power to the device. This procedure extends the data retention of nonpowered SRAM cells to the millisecond timescale. However, the temperature monitoring provided by the DS36xx family would interpret this action as a tampering event, and the device would erase its internal memory before the onset of this cryogenic memory-retention effect. The memory is hardwired to provide a high-speed-clear function that completely resets the entire memory array in less than 100ns. This function can also be triggered by other tamper events (such as an interlock breech) or through a direct command sent to the device's I²C-/SPI™-compatible interface.

The DS36xx devices also include a proprietary feature called nonimprinting key memory. Specifically, nonimprinting key memory addresses the security risk created by the tendency of SRAM memory cells to exhibit charge accumulation or depletion (depending on the data that is stored) in the oxide layers of the devices composing the memory cells. Data stored in these conventional memory cells over a long period of time causes oxide layers to become stressed, and subsequently leaves an imprint of the data that was stored there. This data can be read even after the cells have been cleared.

However, nonimprinting key memory technology has been designed and developed to eliminate the phenomenon of oxide stress. The technology works by continuously complimenting the device's conventional battery-backed SRAM memory. Therefore, when the memory is cleared as a result of a detected tamper event or through a direct command, the entire memory is cleared and no trace of the data that resided there will be present. This function offers the designers of military and government products a unique and extremely secure method for storing highly sensitive encryption keys.

Response to Tamper Events

The DS36xx devices constantly monitor all of the previously described tamper inputs and events. When tampering is detected, either through the internal or external tamper-detection mechanisms, a tamper response is immediately generated. The tamper event starts with identification of the tamper source. The tamper latches remain frozen until the condition causing the tamper event has been cleared. Then the tamper latches a reset. **Table 1** outlines the specific sequence of actions taken by the DS36xx devices during a tamper response.

Table 1. Sequence of Actions Taken when a DS36xx Device Detects a Tamper Event

Step	Action
1	The internal encryption key is immediately, completely, and actively erased (if applicable).
2	The external RAM is erased (if applicable).
3	The tamper-latch registers record the state of the tamper input sources.
4	The tamper output asserts to alert the system processor.
5	The tamper-event time-stamp register records the time of the tamper event.

Supporting Secure Military Applications

In addition to the physical security needed to protect a stored encryption key, physical security is also needed in the actual generation of an encryption key. That is, the method used to generate a digital encryption key must ensure that an unauthorized copy of the key cannot be regenerated, either by the same equipment (which would defeat the purpose of secure data storage provided by the DS36xx family), or by an exact replica of the equipment.

The random-number-generator (RNG) function of the DS36xx devices is a deterministic pseudorandom algorithm, which is seeded using two sources of natural randomness generated on chip. This function provides a continuous bitstream that is intended to be post-processed by the host CPU to form the seed for a certified software RNG function. Furthermore, each DS36xx secure supervisor contains a factory-programmed unique silicon serial number, which is readable through the I/O port. The silicon-inscribed serial number offers the user a method to uniquely identify each end product.

Additionally, the newer DS36xx devices can erase certain specific memory cells based on the type of tamper that occurred. This function is referred to as erasure hierarchy (see **Table 2** for devices), and is useful for applications in which the integrity of the equipment is still intact. That is, one can still use the equipment to a certain degree after the tamper has occurred, though all of the functions may not be available. One such application is a communications device, such as a secure military radio, that must remain somewhat operational although a tamper event has occurred.

Table 2. DS36xx Devices and Their Distinctive Features

Part	I/O	No. of Analog Voltages Monitored	No. of Digital Inputs Monitored	Operating Temperature Range (°C)	Internal Key Memory (Bytes)	External Memory Control	Random Number Generator	Overvoltage Monitor	Battery Monitor	Erasure Hierarchy
DS3600	3-wire	4	1	-40 to +85	64	√	√		√	
DS3605	I²C	4	1	-40 to +85	N/A	√	√		√	
DS3640	I²C	5	3	-40 to +85	1k		√	√	√	

DS3641	4-wire	5	3	-40 to +85	1k		√	√	√	
DS3644	I²C	12	4	-55 to +95	1k	√	√	√	√	2 levels
DS3645	I²C	12	4	-55 to +95	4k	√	√	√	√	
DS3650	4-wire	2	N/A	-40 to +85	N/A			√	√	
DS3655	I²C	N/A	4	-40 to +85	64					
DS3665*	SPI	12	4	-55 to +95	8k	√	√	√	√	4 levels

Besides providing high levels of data security, many defense applications are also required to withstand a wide temperature range during both operation and storage. While the DS36xx devices are intended to provide high security in conventional ambient operating environments, some of the newer products in this family also support wider operating temperature ranges that approach the extremes defined by the full military temperature range (-55°C to +95°C for the DS36xx versus -55°C to +125°C for the full military range).

Conclusion

As shown in Table 2, the DS36xx family of secure supervisors provides a wide range of capabilities, enabling systems that can generate and store encryption keys, monitor for tamper events, and actively and completely destroy the keys when a tamper event is detected. Additionally, by making use of the external inputs provided by the DS36xx devices, the system designer can add more layers of security to an application to meet the requirements set forth in mandates relating to the FIPS, NSA, and WIN-T.

*Future product—contact factory for availability.

General Dynamics is a registered trademark and registered service mark of General Dynamics Corporation.
Secure Computing is a registered trademark and registered service mark of McAfee, Inc.

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 4185: http://www.maximintegrated.com/an4185
APPLICATION NOTE 4185, AN4185, AN 4185, APP4185, Appnote4185, Appnote 4185