

Addressing the physical security of encryption keys

Physical security of an encryption key 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.

By Swati Joshi

The essence of secure communications is protecting the encryption key. While large encryption keys can provide a degree of protection against brute-force computational techniques to break a code, this measure does not address physical security, which is equally important. To address this need, several facets of physical security must be considered. These include a 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 includes protection against clandestine physical and mechanical probing.

Using features that range from package design, to external-sensor interfaces, to internal circuit architectures, special components (members of the DS36xx family of secure supervisors from Maxim) can provide all these capabilities to military electronics design engineers. This can simplify compliance with security requirements for mature and emerging portable military computing and commu-

nities systems. The range of possible applications for these devices is diverse (Figure 1).

Security for electronic data

FIPS, which stands for Federal Information Processing Standard, describes the U.S. government's requirements that IT products must meet for sensitive, but unclassified uses. These standards are published by the National Institute of Standards and Technology (NIST). The FIPS 140.2 standard can be found at <http://csrc.nist.gov/publications/PubsFIPS.html>. The FIPS 140.2 standard has four basic levels:

Level 1. No physical security mechanisms required.

Level 2. Tamper-evident physical security.

Level 3. Tamper-resistant physical security.

Level 4. Physical security provides an envelope of protection.

For advanced-security military communication applications, designs must meet NSA type 1 certification standards. Equipment certified by the National Security Agency

(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; and
- 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), the tactical communications protocol for warfighters. WIN-T supports a range of data, voice and video capabilities. This network helps the soldier stay connected at all times from any location by providing mobile, reliable, high-bandwidth communications. The capabilities provided by WIN-T are delivered by using popular communications technologies, like Wireless LAN, voice-over IP, and third-generation cellular/satellite technology. WIN-T links warfighters located in tactical ground units with their commanders throughout the 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 "bolted on" as an afterthought. This ensures safe and secure transmission of voice communications and digital data across the network.

In the past, systems were designed for speedy deployment, leaving security functions to be implemented as upgrades in the field. This was because built-in security functions were considered to be more expensive and a cause of schedule delays. However, all military communication applications now require a higher level of security from the start in order to provide

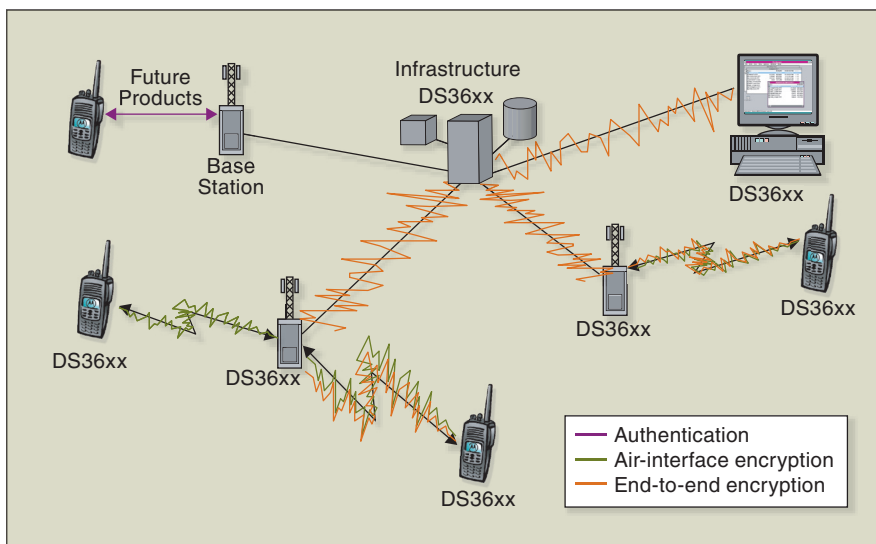


Figure 1. The capabilities of the DS36XX are suited for a range of present and future military and homeland security communications functions, including secure communications and client authentication.

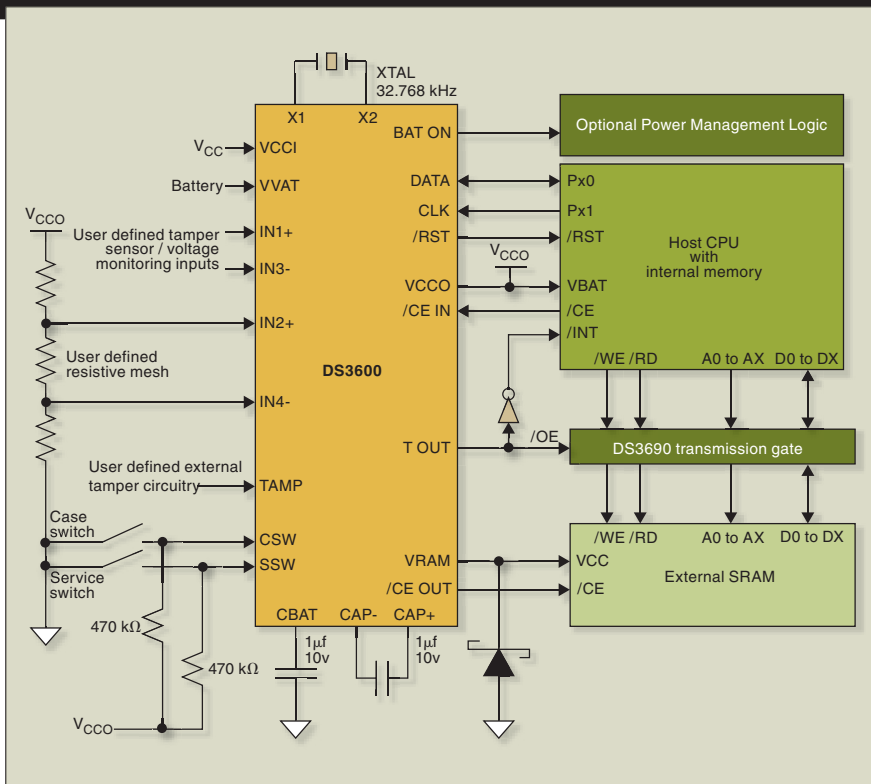


Figure 2. The DS3600 secure supervisor uses a combination of features and mechanisms to detect tampering and protect the contents of battery-backed volatile memory, such as internally stored encryption keys or other sensitive data stored in an external SRAM.

enhanced interoperability, connectivity and regulatory compliance with FIPS 140.2, NSA and WIN-T. Security and intrusion prevention are increasingly crucial factors for other military applications as well (for example, General Dynamics with Secure Computing has developed the MESHnet Firewall for use in battlefield vehicles).

As a result, new military communications systems or components will no longer be released without meeting the applicable standards. Typically, military applications require, at a minimum, a level-3 certification for FIPS 140.2. Specifically, military communication applications are required to meet, at a minimum, FIPS 140.2 levels 3 and 4. Furthermore, in higher-level applications, these applications must adhere to NSA type-1 and/or the newly implemented WIN-T requirements.

Achieving compliance with security requirements

However, addressing these 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 become more stringent over time. Keeping abreast of the ever-changing security standards can become troublesome for designers. This is because the design process must be guided by 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 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 physical security enhancement.

When designing secure military systems that meet FIPS 140.2 (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 the Maxim DS36XX series, such as the DS3600 shown in Figure 2, offer integrated solutions to secure encryption keys and critical data by actively detecting tamper, 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 by the device, and when it falls below the low threshold, an external backup battery is instantly and automatically switched in to keep the internal and external protection circuitry alive. Thus, tamper detection is not interrupted with the loss of the main power source to the equipment.

In order to comply with the requirements of FIPS 140.2 (levels 3 and 4), as well as the NSA type 1 and WIN-T specifications, tamper

SMALL; LIGHT; EFFICIENT

ATS Series DC-DC Converters



Features:

- 16V to 50V DC Input Range
- Internal EMI Filter
- High efficiency to 82%
- -55°C to +125°C Operating Temperature Range
- Low weight: 77 grams (typical)

With an integrated MIL-STD-461 compliant EMI input filter, IR's ATS series of 25W single and dual output DC-DC converters offer significant space and system cost-savings for high reliability and aerospace applications.

For more information call
1.800.919.7898 or visit us at
www.irf.com/hirel

International
IOR Rectifier
THE POWER MANAGEMENT LEADER

detection components must have the ability for designers to attach their own external sensors, so that an envelope of protection—that is, the security boundary—can be provided around the devices storing the protected data. The ability to attach external sensors to the DS36xx series gives the system designer 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.

In keeping with these requirements, analog supply voltages, digital signals, and a resistive-mesh protective sensor grid can all be easily and simultaneously monitored by DS36xx secure supervisors. Furthermore, all DS36xx devices are offered in chip-scale ball-grid-array (CSBGA) packages, as shown in Figure 3. This provides another layer of passive physical security of the control and data signals by severely restricting access to the pins of a mounted device.

Internal security features

The DS36xx device family includes additional layers of protection in the form of internal tamper-detection mechanisms. These internal mechanisms complement the device family's ability to interface to a customized configuration of external tamper-detection sensors. The internal tamper-detection mechanisms, which include the on-chip temperature sensor, case-switch monitor, power-supply monitor, battery monitor, and an oscillator monitor, provide continuous tamper-detection monitoring. This monitoring remains active at all times, especially when running on battery power in the absence of main 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 the certification bodies, such as the NSA, and those governing the FIPS and WIN-T standards, the designer can make use of the internal temperature sensor, which monitors the substrate temperature. Once the upper or lower temperature limits are violated, a tamper response is initiated by the device.

In addition to the measurement of the instantaneous temperature, a temperature-monitoring function is provided in the DS36xx family. Specifically, a rate-of-change detector monitors the speed at which the substrate temperature changes, and a rapid increase or decrease in temperature will trigger a tamper response in the device. This provides more protection against advanced clandestine data-recovery techniques.

For example, one documented method of recovering data from protected SRAM involves the application of liquid nitrogen

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.

Table 1. Sequence of actions taken when a tamper event is detected by the DS36xx family.

prior to the removal of power to the device, which extends the data retention of unpowered SRAM cells to the millisecond time scale. 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 resets the entire memory array in less than 100 ns. This function can be triggered by other tamper events (such as an interlock breach), or via a direct command sent to the device's I²C/SPI interface.

The DS36XX devices include another feature—referred to as non-imprinting key memory (Maxim is pursuing a patent on this technology)—that relates to another vulnerability inherent in conventional SRAM memory cells. Specifically, this feature addresses the security risk created by the tendency of these 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 will cause oxide layers to become stressed, and will subsequently leave an imprint of the data that was stored there. This data can be read even after these cells have been cleared.

However, non-imprinting key memory technology has been designed and developed to eliminate the phenomenon of oxide stress. The technology works by the continuous complementing of the device's conventional battery-backed SRAM memory. Therefore, when the memory is cleared as a result of a detected tamper event, or via 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 secure method for storing highly sensitive encryption keys.

Response to tamper events

The DS36xx products constantly monitor all of the previously described tamper inputs and events. When tampering is detected,



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.

either via 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 will remain frozen until the condition causing the tamper event has been cleared and the tamper latches reset. Table 1 outlines the specific sequence of actions taken by the DS36XX devices during a tamper response.

Supporting secure military applications

In addition to the physical security needed to protect a stored encryption key, there is a need for physical security in the 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 is a deterministic pseudo-random algorithm, which is seeded using two sources of natural randomness generated on chip. It provides a continuous bitstream, which 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 by using the internal serial number.

The newer DS36XX devices have the ability to erase certain specific memory cells based on the type of tamper that has occurred. This function is referred to as erasure hierarchy, and is useful for applications where the integrity of the equipment is still intact. That is, one can still use the equipment to a certain degree after the tamper

Advertiser Index

COMPANY NAME	WEB SITE	PAGE#
Aethercomm	www.aethercomm.com	5
International Manufacturing Services	www.ims-resistors.com	7
International Rectifier	www.irf.com/hirel	13
Locus Microwaves	www.LocusMicrowave.com	2
M/A-Com, Inc.	www.macom.com/defense	IFC
MITEQ	www.miteq.com; www.mcl.com	BC
Rohde & Schwarz	www.test-rsa.com/FSU67/DE1007	IBC

Continued from page 14

Part Number	I/O	Analog Voltages Monitored	Digital Inputs Monitored	Operating Temperature	Internal Key Memory	External Memory Control	Random Number Generator	Over-Voltage Monitor	Battery Monitor	Erasure Hierarchy
DS3600	3-wire	4	1	-40 °C to +80 °C	64 Bytes	Yes	Yes	No	Yes	No
DS3605	I ² C	4	1	-40 °C to +80 °C	N/A	Yes	Yes	No	Yes	No
DS3640	I ² C	5	3	-40 °C to +80 °C	1 kBytes	No	Yes	Yes	Yes	No
DS3641	4-wire	5	3	-40 °C to +80 °C	1 kBytes	No	Yes	Yes	Yes	No
DS3644	I ² C	12	4	-55 °C to +95 °C	1 kBytes	Yes	Yes	Yes	Yes	2 levels
DS3645	I ² C	12	4	-55 °C to +95 °C	4 kBytes	Yes	Yes	Yes	Yes	No
DS3650	4-wire	2	N/A	-40 °C to +80 °C	N/A	No	No	Yes	Yes	No
DS3655	I ² C	N/A	4	-40 °C to +80 °C	64 Bytes	No	No	No	No	No
DS3665	SPI	12	4	-55 °C to +95 °C	8 kBytes	Yes	Yes	Yes	Yes	4 levels

Table 2. Members and features of the DS36XX family.

has occurred, even though all the functions may not be available. One such application is a communications device, such as a secure military radio, that must remain operational to a certain degree, even though a tamper event has occurred.

Besides providing high levels of data security, many defense applications are required to withstand a wide temperature range during operation as well as storage. While the DS36xx family is intended to provide high security in conventional ambient operating environments, some of

the newer products in the family support wider operating temperature ranges that approach the extremes defined by the full military temperature range (-55 °C to +95 °C for the DS36xx vs. -55 °C to +125 °C for the full military range).

As shown in Table 2, the DS36XX family of secure supervisors provides many 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. By making use of the

external inputs provided by the DS36xx products, 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. **DE**

ABOUT THE AUTHOR

Swati Joshi is the business manager for NVSRAMs and secure supervisors at Maxim Integrated Products. Joshi holds a B.S. in chemical engineering.