Keywords: pci pts 3.1, pci ped, maxq1850, security, two-chip, payment terminals, financial terminals, certification

APPLICATION NOTE 4809

Designing Next-Generation Payment Terminals That Meet PCI PTS 3.x Requirements

May 19, 2011

Abstract: Designing enhanced yet secure payment terminals is discussed in this application note. We expose the pitfalls that manufacturers face for PCI-PED PTS certification and explain how they can be addressed and solved by the use of two-chip architecture, based on the DeepCover® Secure Microcontroller (MAXQ1850).

A similar version of this article appeared in the March-April 2011 issue of *CardsNow! Asia Magazine*.

Card-based transactions are soaring, with over 110 billion worldwide in 2009. This expansion has several causes. Increasingly global payment schemes guarantee broad acceptance, and the available technologies and standardization efforts are making transactions more reliable, convenient, and inexpensive for merchants. Perhaps the most important factor, however, in the success of card-based transactions is the growing confidence of cardholders in the payment system—from the initial purchase, to the debit, and beyond.

New Terminals, New Trends

Financial terminals have become the vehicle for delivering a range of new services from payment-products companies. Terminals are no longer simple card-reading machines. They have become sophisticated computing devices capable of performing transactions, managing inventories, and running business applications. This changing role is clearly indicated by the new terminology used to describe terminals: formerly known as point-of-sale (POS) devices, they are now called point-of-interaction (POI) systems. POI systems must now communicate faster and more easily (e.g., with USB, Ethernet, Wi-Fi®, or Bluetooth®). They must support several concurrent applications and handle a plurality of card types (payment cards, loyalty cards, etc.).

Also changed are the conditions of use. POIs must sometimes operate in moist environments, either outside or inside. They are frequently portable and ergonomic, sporting visually appealing form factors that complement the merchant's image. Widespread reuse of available technologies makes the terminals look and feel like the everyday devices with which we are familiar, such as smartphones, notebooks, and gaming consoles. Modern POIs employ similar design aesthetics, feature rich color displays, use sophisticated touch-screen interfaces, and offer connectivity features that facilitate their integration into information systems. Full exploitation of these hardware technologies enables software reuse as well, from off-the-shelf operating systems to software stacks that allow abstraction of hardware layers. In general, software reuse speeds development, reduces validation risks, and provides faster time to market with lower R&D costs.

Terminal Security

The main difference between POI terminals and consumer electronics (CE) devices is the need for high levels of security. The global deployment of EMV* cards means global threats. Attacks can be executed quickly and globally if appropriate countermeasures are not in place. Furthermore, the expenses incurred in making an attack (in terms of tooling, time spent, etc.) can be higher because the return on investment is higher. For that reason, the largest threat to security is now considered to be crime syndicates.

The interactive features, multiple communication interfaces, and advanced services offered by today's complex financial terminals all serve as potential open doors for attackers. As a response, coordinated efforts have been made to adapt those advanced services to the security levels necessary to ward off attacks. The Payment Card Industry Security Standards Council (PCI SSC) was founded by the major payment-products companies—American Express, JCB, MasterCard, and Visa—to standardize security efforts across the industry.

The PCI SSC developed a standard called PIN Transaction Security (PCI PTS) to define the requirements for financial terminal security. Formerly known as the PCI PIN Entry Device (PCI PED) standard, PCI PTS addresses the physical and logical attacks that attempt to extract PIN codes and encryption keys from POI systems. Based on both field experience and laboratory research, PCI PTS outlines security mechanisms for every kind of attack: physical tampering, environmental modifications, software-interface attacks, cryptanalytic attacks, and threats to the security policies set up by the manufacturer (keys management, version-control system, organization, and security management). PCI PTS strives to protect PIN codes as long as they are in plain-text format within the terminal, or on their path to the smart card.

Physical requirements prevent attackers from opening the terminal and inserting a PIN-recording device, from capturing electromagnetic emanations when a PIN is entered or transmitted, or from modifying the terminal's behavior. Logic requirements prevent attackers from modifying the card reader and from taking control of applications running on the terminal, for the purpose of retrieving, recording, or transmitting PIN codes and other sensitive data.

Additional requirements safeguard the magnetic-stripe (magstripe) data. Every PCI PTS requirement corresponds to a specific category of attack, and is associated with a minimal required level of resistance, which is represented by a numeric value ranging from 16 to 35. To pass a designated requirement, the payment terminal must demonstrate a resistance commensurate with the minimum attack potential, also known as the attack value.

This attack-value approach is inspired by ITSEC's Joint Interpretation Library for smart cards, and is based on target knowledge, attack duration, and the attacker's resources and expertise. Each of these categories includes several levels, and each level is rated a certain value. In considering an attack, the sum of values from each category characterizes the attack value. For example, the documentation category includes three levels: public, restricted, and secret. If a particular incident involves an attack on restricted documentation, then the value of that level (restricted documentation) is added to the attack sum.

An estimation of resistance to each requirement is performed by an accredited security laboratory, and the final decision regarding approval (of a terminal, for instance) remains with the PCI PTS members. Because payment terminals are accessible to attackers, PCI PTS specifies levels of protection against the many threats to sensitive cardholder data. PCI PTS does not provide solutions to such exposure, so it is up to the manufacturer to decide how to meet the security requirements. Terminal manufacturers will face even more challenges now that the security requirements of PCI PED 2.1 have been superseded by those of PCI PTS 3.1 (as of March 2012).

PCI PTS 3.x

The PCI security requirements for payment terminals contain important improvements, and have been strengthened to resist the most recent threats. Alternatively, its new approach fosters a modular development that can simplify the business of manufacturing. This evolution is indicated by the change of terminology from PIN Entry Device (PED) to POI device, which reflects the change of use. Terminals perform financial transactions as before, but they now do more than that, and the new terminology shows manufacturers that PCI SSC has considered this expansion of capabilities.

From a process point of view, the certification has been simplified to propose a single evaluation covering all categories of devices (POS, EPP, vending machines, kiosks), organized as two mandatory evaluation modules: device core requirements and device integration requirements. Also proposed are two new optional evaluation modules.

From a security point of view, the requirements have been slightly modified and strengthened based on feedback from the field. The major requirements have had their attack values increased from one to two points, especially those related to physical tampering (the keyboard, magstripe, and card slot). The attack-cost values now range between 16

and 35 (vs. 14 and 35 under PCI PED 2.1). In addition, the rule for passing a given requirement is now tougher. The older standard required only that the sum of attack-preparation and attack-exploit values equal a minimum number; now the attack-exploit value by itself must have a minimum. (Preparation is the identification phase in which the attacker studies the problem, devises a method, and tests his equipment. In the exploitation phase, the attacker goes to a public place and makes an actual attempt to steal data.)

Other new requirements clearly address the new POI architecture and services. As an example, requirement B17 considers the context of multiple applications hosted on the same terminal, which fully reflects the software architecture of modern terminals. Another example is the creation of the new optional evaluation modules: the Open Protocols module deals with security over open/public networks, and typically addresses security issues coming from an IP-connected terminal, similar to the threats faced daily by a PC. The Secure Reading and Exchange of Data (SRED) module defines requirements for protecting cardholder account data within the terminal. **Table 1** lists the most demanding security requirements, as well as the functional requirements for efficient, cost-effective terminal design.

Table 1. Security and Functional Requirements for PCI PTS

Category	Requirement	Typical Solutions
PCI PTS	Fast erasure of data (A1) in response to tampering	Four sensor inputs are available; automatic erasure is guaranteed 24/7
	Detection and countering of environmental perturbations	Glitch protection; temperature control
	Cryptographic services that use standardized algorithms	Supported algorithms valid for future: SHA-2, AES; supported key lengths up to very secure values (2048 bits for RSA, 256 bits for AES, 168 bits for 3DES)
	Side-channel countermeasures for cryptographic implementation	Hardware and/or software countermeasures already implemented
	Secure communications	Any mutual authentication-based communications using session keys and challenge/response protocols
	Strength of random numbers	Pass the NIST tests
	Control of sensitive peripherals by secure processor	Every sensitive peripheral is under control of the secure processor
	Control of prompts on display	Public-key cryptography services; security policy for signature prompts
	Protection of sensitive services, keys	No data leaves the secure processor
Power consumption	Energy savings	No dilemma between energy and security
	High-performance security applications	Powerful processor; smart interrupts management
	Easy development and debug features	Efficient tool chain supporting modern languages; user libraries
	Aggressive designs that require fewer and fewer chips on PCBs	No additional external memory required; PCB routing is simplified

Ease of integration	Aggressive designs that require smaller PCBs	Very small footprint addressing very important functions
	Sped-up development of security applications	No risk for lack of countermeasures; no risk for lack of validation
	Limiting the risk of security weakness	Easy configuration avoids risk of misuse
	Battery-backed data memory	Allow storage of secrets and other data requiring long-life storage (transaction data, DUKPT keys, etc.)
	Accurate source of time	Strong support (application notes, reference designs, EV kits)
BOM cost	Fewer chips, which reduce BOM cost by integrating more functions	Integrated IPs in single chips

Managing the Expense of Security Measures

Terminal manufacturers face the challenge of designing powerful, stylish POIs that meet stringent security requirements. However, developing and maintaining security expertise internally is an expensive chore that requires a dedicated team of experts and significant R&D resources. This burden poses a substantial barrier to entry for newcomers, yet it does not provide established manufacturers with a competitive advantage. Security certification, after all, is mandatory for all payment terminals.

Standardization has therefore created a market for security modules from specialized commercial vendors. Because certification is not a differentiating feature, manufacturers are free to use off-the-shelf security products to satisfy certification requirements. These products offer several advantages over those developed internally.

They enable terminal manufacturers to focus on value-added features. Security is not a specialized feature, but rather a standard and fundamental requirement of all terminals. By forming partnerships with security vendors, a manufacturer is able to focus on adding value to its financial terminals.

Improved cost efficiency allows the development of sophisticated security mechanisms. Because R&D costs are shared by multiple customers, the security-product manufacturer is able to develop advanced technologies that are beyond the reach of individual terminal manufacturers. Advanced technologies make security mechanisms more efficient by fostering deeper integration. Such economies of scale are increasingly important as security requirements become more complex. Indeed, we need specialized security vendors who have the expertise to propose effective countermeasures.

The use of approved modules reduces risk and speeds POI qualification. By performing security evaluations and obtaining PCI PTS approval for off-the-shelf security products, the module manufacturer reduces development risks for the terminal designer. This complementary effort simplifies security integration and speeds terminal qualification.

Overview of Security Architectures

Three main architectures govern today's payment terminals. They differ in the way that security services are accessed, that assets are integrated with other features in the terminal, and that requirements are addressed (see Table 1).

Security Managers

The first terminal architectures used a security manager to add security to a general-purpose µC. The security manager safeguards sensitive credentials and detects physical or environmental tampering (e.g., changes to temperature or voltage). It also guarantees protection of the keys storage by providing external sensor inputs, which in turn allows connection of a security cover, PCB mesh, and tamper sensors (**Figure 1**).

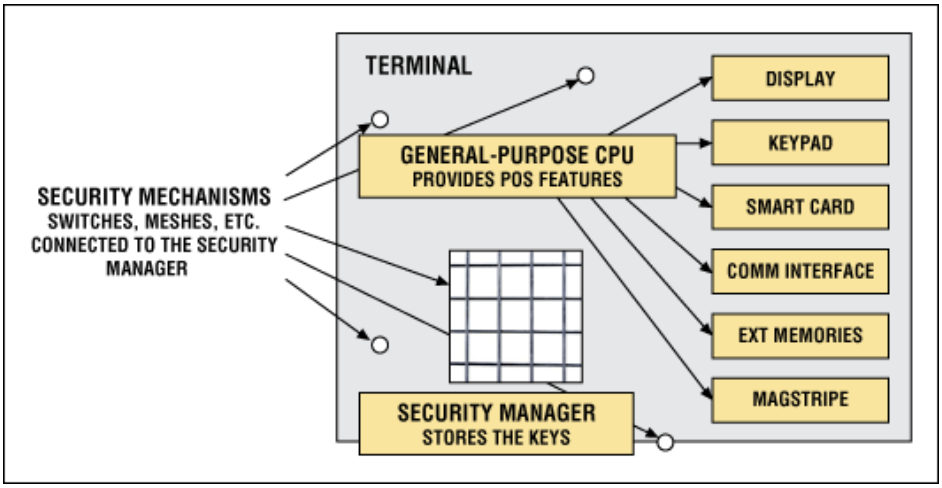


Figure 1. This payment-terminal architecture is based on a security-manager IC.

Security managers such as Maxim's DeepCover® Security Manager (DS3600) employ a patented, nonimprinting memory architecture that stores the encryption keys in on-chip nonvolatile (NV) SRAM. This battery-backed memory eliminates the problem of memory imprinting due to oxide stress, and thereby prevents the possibility of hackers passively detecting the data remnants in stressed memory cells. When intrusion is detected, the chip instantly and completely erases the NV SRAM content. Additional security services such as random-number generation can be found on these security managers. All remaining services and functions are performed by the general-purpose microcontroller (µC), including cryptographic services and sensitive-interface controls.

Two-Chip Architecture (Two Microcontrollers)

A second approach is to split the computing and security functions between a general-purpose µC and a secure companion chip (**Figure 2**). The general-purpose µC performs all nonsecurity-related tasks, while the secure coprocessor, which also contains a µC, controls each sensitive interface, performs the cryptographic computations, and behaves as an alarm system.

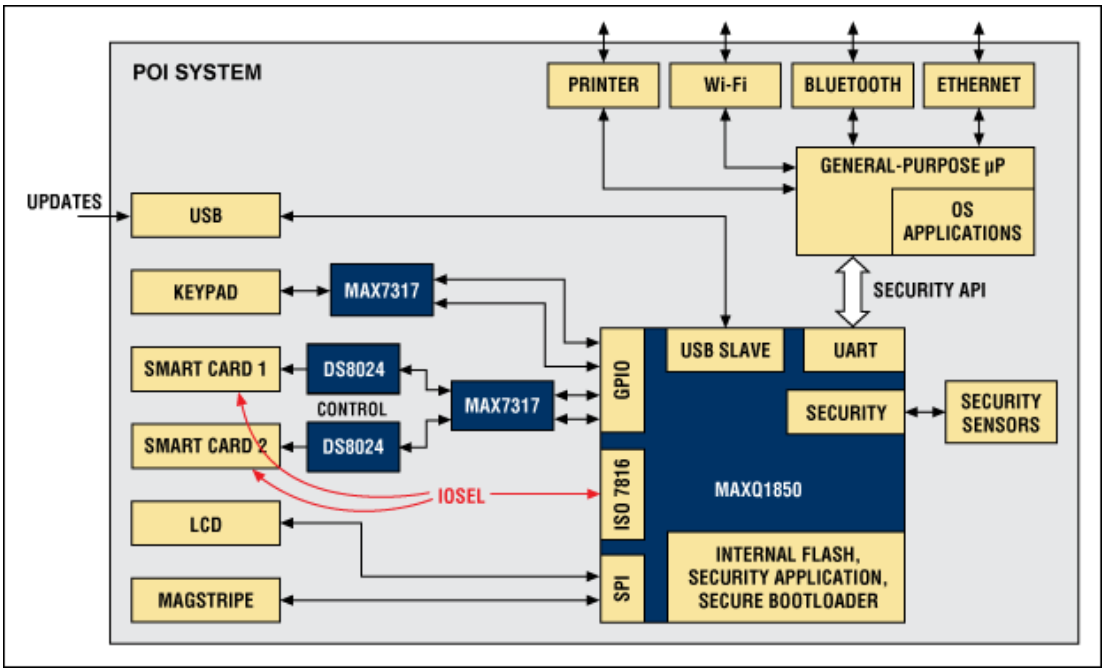


Figure 2. The two-chip architecture combines a general-purpose µC with a secure µC.

The interface between the two µCs is specifically controlled to prevent leakage of sensitive information. This architecture is particularly well suited for modern POI designs that use off-the-shelf products for meeting the PCI PTS requirements. You can select a general-purpose µC solely on functional criteria such as performance capabilities, connectivity, and computing power, and let the secure µC handle all security functions, such as PIN and key management, battery backup for memory, tamper detection, and cryptographic computation. By allowing use of preapproved off-the shelf devices, you can select this µC purely according to the requirements for achieving PCI PTS security approval.

Secure Companion Chip

One such chip, the 32-bit DeepCover Secure Microcontroller (MAXQ1850), is designed as a companion to any general-purpose µC. It addresses the most stringent PCI PTS requirements, as indicated by its security evaluation report:

- Physical tamper protection is provided by tamper-response sensors connected to a battery-backed memory, which is instantly erased upon tampering
- Strong protection against faults and environmental perturbations (glitches, extreme temperatures, etc.)
- Sensitive assets (keys and firmware) hosting by embedded memories
- Die-shield protection of embedded memories
- Secure cryptographic implementation of all required algorithms (side-channel countermeasures)
- Secure random source for key generation
- Direct control of sensitive peripherals (e.g., smart card, keypad, and display)

The MAXQ1850 addresses the key security and design requirements of Table 1. Its high-performance RISC core, low pin count, and integration of critical blocks make it well suited for a range of POI systems, including portable devices with ultra-small form factors. Figure 2 shows how the MAXQ1850 eases the design of POIs that have a two-chip architecture.

- The I/O-select mechanism on the smart-card interface allows the system to manage two cards using only one interface, while the smart-card interface chips (DS8024) are controlled through the SPI ports.
- The SPI ports are shared between the smart-card interface and the LCD, using the GPIO as a chip select.
- The cascaded SPI-to-GPIO converters (MAX7317) ease management of the reconfigurable GPIO/SPI ports for accessing peripherals in parallel. This configuration uses the GPIO as chip selects for the magstripe reader, keypad, etc.
- The USB link connects the secure µC and the general-purpose µC for interfacing through a security application programming interface (API).

Integrated Secure µCs

The third approach, in wide use for securing financial terminals since the PCI PED certifications arose, is to choose a single-chip architecture that incorporates a highly integrated, high-performance secure µC (**Figure 3**). Like general-purpose microcontrollers, these µCs are fabricated using the most recent semiconductor technologies; feature several communication interfaces such as USB, SPI, and smart card; and are able to run feature-rich operating systems such as the Linux® OS. They embed modern processors running at high frequencies, and are able to manage large external memories such as NOR and NAND flash, as well as various kinds of RAM.

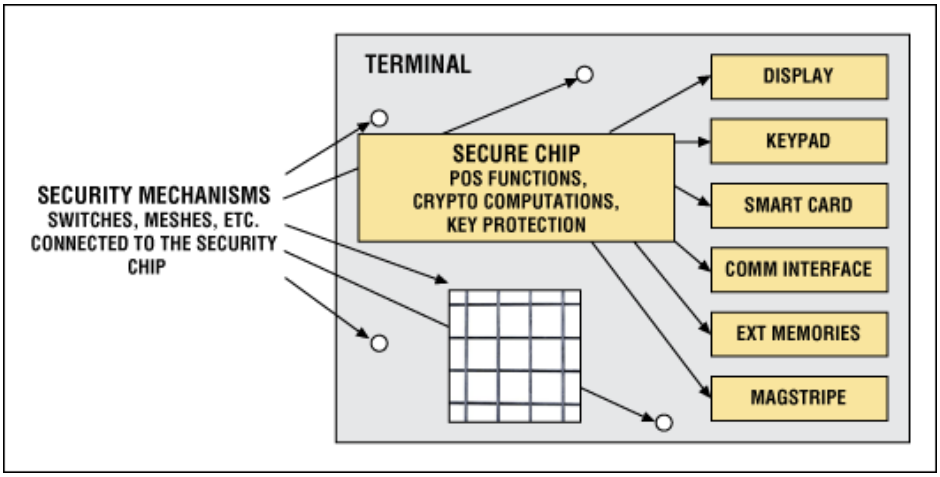


Figure 3. The most compact terminal architecture incorporates a single µC that includes all the necessary security measures.

Like security managers, these devices embed secure NV SRAM and tampering/monitoring sensors. Like companion chips, they run secure cryptographic algorithms such as 3DES, AES, and RSA, which are resistant to both differential power analysis (DPA) and simple power analysis (SPA). This high level of integration provides many benefits, both on the security side and on the bill-of-materials (BOM) side.

Security mechanisms are integrated at the level of silicon, and on a scale for which attacks can only be sophisticated ones. Integration guarantees a full chain of trust for startup, and also for emergencies and alarm situations—the alarm signal cannot be cut off. Because critical functions have already been gathered in the chip, it decreases the design risk of bad integration due to the introduction of weak links. It also avoids the need for an additional security enclosure when using the integrated, on-the-fly, external-memory-encryption engine.

Software security also benefits from this integration, because security mechanisms rely on hardware-intensive, standardized mechanisms such as a memory-management unit (MMU). Note that the separation between sensitive and nonsensitive applications is performed at the software level in a single-chip approach, but at the hardware level in a two-chip architecture. Software separation is currently implemented in three different ways, none of which is exclusive. The first uses a "hypervisor" that splits secure and nonsecure applications into separate containers. The second uses an operating system such as Linux, which splits applications directly, and the third uses Java® software or a Java-like virtual machine to handle separate secure applets.

All-in-one integration simplifies the terminal design by lowering the required number of chips, reducing the PCB footprint, and permitting the use of more appealing form factors. It also speeds development by requiring only a single tool chain and supporting only one µC core. Among other suppliers, Maxim offers a variety of highly integrated, 16- to 32-bit secure µCs running at clock speeds as high as 200MHz.

When selecting a secure µC, you should choose one that comes with a security evaluation report performed by a PCI PTS laboratory. This report provides the confidence that comes with a completion of full laboratory testing, in which the results reveal both the chip vendor's level of expertise and the level of security obtained with the secure chip. A second consideration is the relative ease of integration in the terminal design. This ease depends on both the µC features and the strength of the vendor's support team. You should look for a µC that integrates key functional blocks such as memory, timekeeping, and tamper sensors, because such integration simplifies PCB routing while supporting the critical security features with a small footprint. Maxim participates in the PCI SSC organization, and is committed to serving the PCI SSC market with state-of-the-art security µCs.

One such µC is the DeepCover Secure Microcontroller (MAX32590) "JIBE", a secure and powerful 32-bit microcontroller, using an ARM926™ core. This low-power device provides superior performance at 400MHz. Its security functions include a 2KB secure memory with instant-erase capability, a secure real-time clock (RTC), and built-in environmental dynamic sensors that detect any intrusion. Volatile and nonvolatile external memories, such as NAND,

NOR, and LPDDR are fully protected by a new, powerful AES-128 encryption/integrity engine. The associated software offer includes a preapproved POI reference design, secure Linux OS, cryptographic libraries, EMV L1 libraries, and PCI PTS assistance.

Reference Design Is PCI PTS 3.x Approved

Maxim's reference design (USIPOS) allows you to build a terminal with the confidence that it will pass PCI evaluation; PCI PTS 3.x approval provides a fast route to getting your terminal certified. Key features of the USIPOS reference design include a meshless architecture, PCI PTS 3.x approval, BOM-optimized hardware, and a secure Linux OS, plus EMV L1 and cryptographic libraries and hardware/software guidelines. You can start with the Maxim design, layout, and BOM, and then customize the design to your enclosure, bringing the completed product to market faster and with less risk and expense.

Security Islands

Beyond the security chip and the assets it handles, other assets—such as the PIN—can be the target of attack. As a precaution, sensors external to the security chip are used to provide protection against physical tampering at the terminal level. The resulting security mechanisms are very efficient and well integrated, with the result that any alarm triggers an immediate erasure of the secure memory. Even so, these sensors are usually monitored off-chip, where the monitoring circuitry can secure other physical areas as well—those in which assets such as the PIN are exposed. To that end, the terminal manufacturer must apply skills and knowledge to correctly implement an alarm-detection mechanism. Alarm propagation and consequence are managed by the secure chip.

Plain-text assets such as the PIN and cardholder-account data are accessible through the keyboard, the magstripe signal, and the smart-card slot. Therefore, these three areas need their own security measures, in addition to those measures employed by the secure chip itself. Assets are only exposed inside these areas, which is why they are called "security islands" (**Figure 4**).

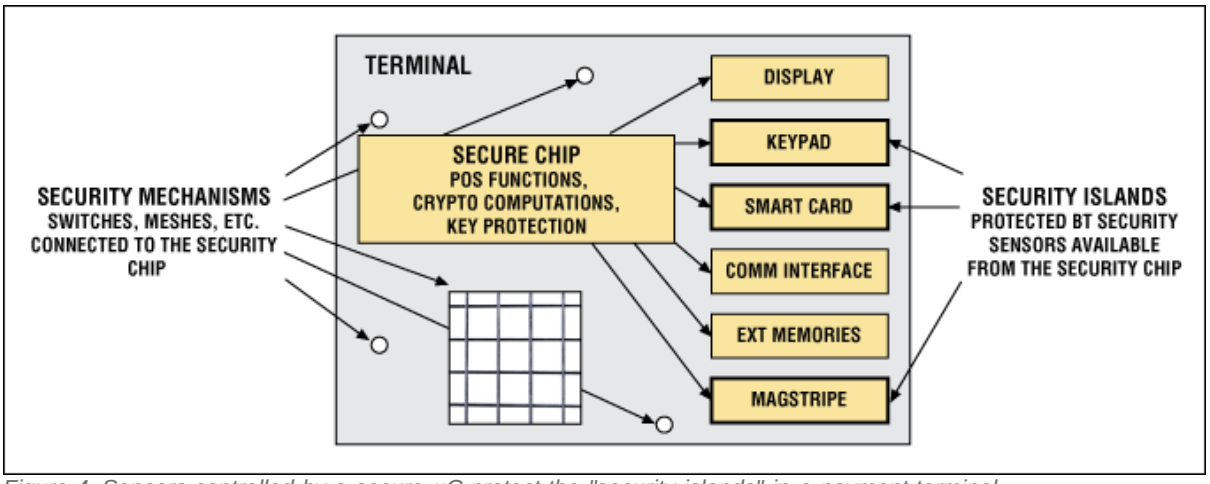


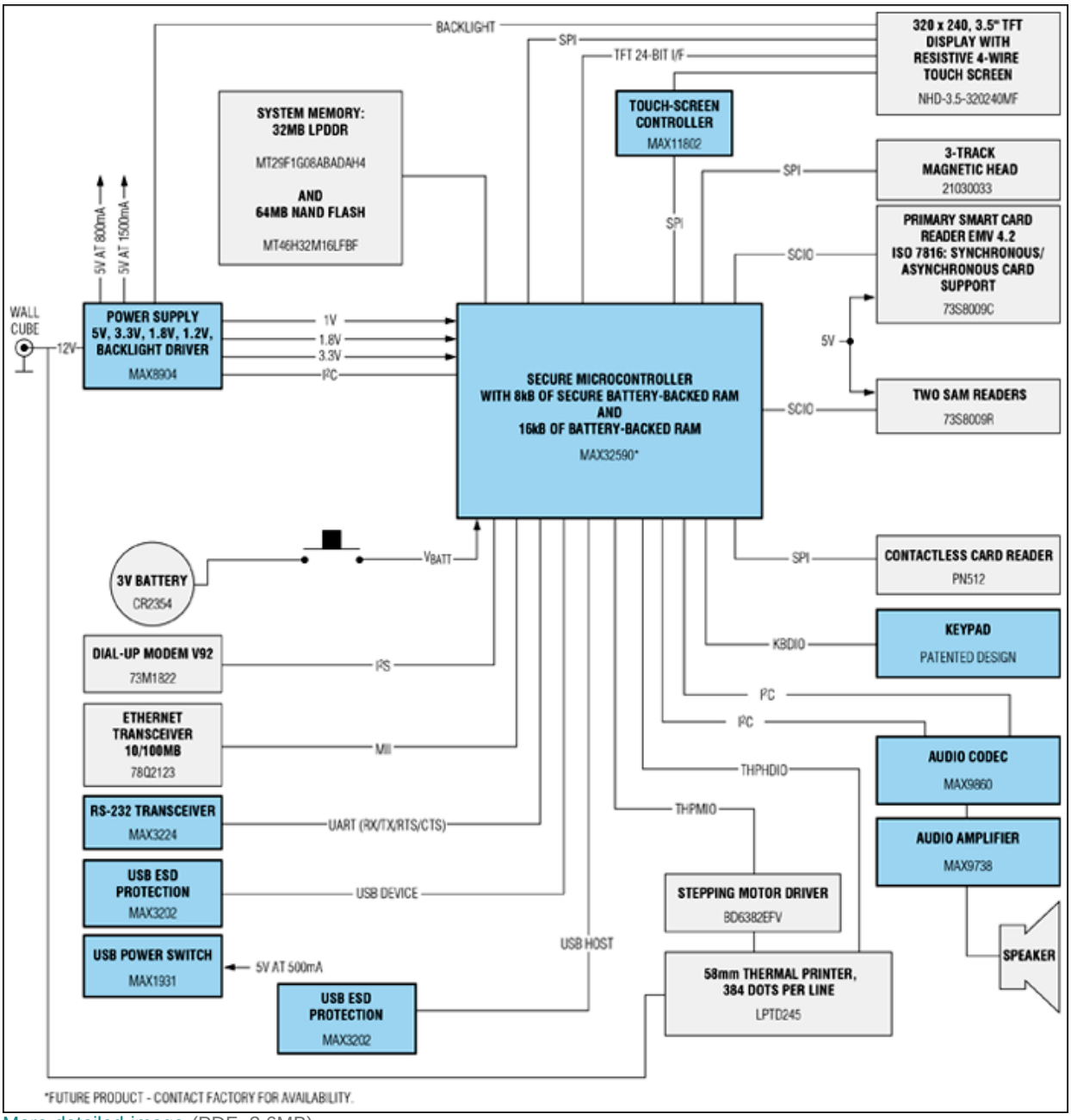
Figure 4. Sensors controlled by a secure µC protect the "security islands" in a payment terminal.

Using the same approach as for off-the-shelf secure chips, some companies are now proposing off-the-shelf designs for some of these secure areas. The most complete solutions are integrated secure smart-card slots such as the C&K secure smart-card slot, and magnetic encrypting heads such as the magneto chipset. These products offer the same benefits—integration, improved security, risk reduction, and cost—as the secure chips mentioned above.

The Ultimate Off-the-Shelf Solution

The full integration of all the above-mentioned off-the-shelf security measures in a single reference design is an important achievement—one that simplifies the terminal manufacturers' product development, certification, and

manufacturing (**Figure 5**). Security is the main issue faced by manufacturers, so an evaluated reference design brings confidence, saves resources, and limits the risk of failure. It also demonstrates compliance with the most demanding security requirements (those of PCI PTS) in an efficient and cost-effective manner.



More detailed image (PDF, 3.6MB)

Figure 5. A block diagram of the JIBEPOS reference design shows the various functions it provides.

Software and Applications

Terminals are made of hardware, but the associated software—no longer restricted to PIN-entry operations—has expanded in recent years to serve a variety of applications. Loyalty and other service-related applications can be found on the devices, and complex software architectures have become necessary to accommodate the graphical interfaces,

the multiplicity of interfaces (Ethernet, USB, GPRS connections), support of EMV, and contactless cards. Strong security measures also impose complexity on the software design: terminals must be attractive, but the security applications must not leak sensitive data, the operating system must control communications between applications, and the cryptographic services must not expose the keys. Still, off-the-shelf software brings many benefits to the terminal manufacturer by saving development time and aiding validation of the final product.

As an example, the Secure Linux operating system, proposed by Maxim and available for the DeepCover Secure Microcontroller (USIP) and DeepCover Secure Microcontroller (MAX32590) "JIBE" platforms, simplifies development and limits the manufacturer's certification risk by providing full compliance with PCI PTS security software requirements. A full Linux offering, it also gives access to improvements developed by that community, including graphical interfaces, peripheral drivers, and communications stacks.

Conclusion

Any of the three architectures described above can produce an enhanced payment terminal without sacrificing security. The ICs mentioned are proven, off-the-shelf devices that increase security, ease integration, and reduce power consumption. Whether used directly, combined with off-the-shelf security islands, or completely embedded in a secure and proven reference design, they improve time-to-market and limit the risk of certification failure. Additional software to complete the solutions is available to manufacturers, enabling them to save time, limit risks, and focus on their core skills.

References

PCI Security Standards Council

MAX32590 data sheet

USIP data sheet

USIP security report: contact your local sales representative

MAXQ1850 data sheet

MAXQ1850 security report: contact your local sales representative

*EMV: A standard produced by the coalition of Europay-Mastercard-Visa, to insure security and compatibility between smart cards (IC cards, chip cards) and associated card readers, POS terminals, and ATMs.

Related Parts		
DS8024	Smart Card Interface	Free Samples
MAX32590	DeepCover Secure Microcontroller with ARM926EJ-S Processor	

	Core	
MAX7317	10-Port SPI-Interfaced I/O Expander with Overvoltage and Hot-Insertion Protection	Free Samples
MAXQ1850	DeepCover Secure Microcontroller with Rapid Zeroization Technology and Cryptography	Free Samples
USIP	DeepCover Secure Microcontroller with MIPS 4KSd Processor Core	
ZA9L1	DeepCover Secure Microcontroller with ARM922T Processor Core	

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 4809: http://www.maximintegrated.com/an4809
APPLICATION NOTE 4809, AN4809, AN 4809, APP4809, Appnote4809, Appnote 4809