Keywords: POS, point of sales, secure microcontrollers, multimedia POS, POS reference design, POS design, POS security, reducing POS design effort, display security, touch screen POS, smart POS

APPLICATION NOTE 5328

Transforming a Smartphone Design into a Sophisticated Point-of-Sale Terminal

By: Christophe Tremlet, Security Segment Manager
Dec 14, 2012

Abstract: Developing a sophisticated and secure point-of-sale (POS) terminal can be a challenge. In addition to security concerns and standards, increasing development costs can put a constraint on designs. This article explains how to design POS equipment with numerous value-added features at a low cost, by taking advantage of the development efforts made by the cell phone industry.

A similar version of this article appeared in Italian in the August 1, 2012 issue of *Elettronica Oggi* magazine.

Driven by the growing trend of smartphones, payment terminals are becoming sophisticated, feature-rich computing devices capable of performing transactions, managing inventories, and running business and social applications. They can deliver advertisements and new services from payment-product companies and provide an enhanced user experience. Advanced features of high-end payment terminals and embedded devices can now include a color touch screen and high-quality audio, and rich operating systems such as the Android® platform. Like smartphones, electronic financial transaction equipment also has the need for multiple connectivity options (i.e., Wi-Fi®, GPRS, 3G) and low power consumption. However, as the complexity of smart equipment systems continues to increase, the development cost is rising even faster. Therefore, developing such advanced devices involves significant design resources and license fees, increasing the potential risk for delays in time to market.

While increasing development costs is a general trend for sophisticated electronic equipment, the increase is even more significant for payment terminals. A major cause for this is simply the difference in volume: development costs for a smartphone are amortized in a reasonable time frame because of the very large number of units that are sold. The Nilson Report estimates that the number of payment terminal sales is only 15 million units per year (much less than the 420 million smartphones sold in 2011[1]). This difference means that the development cost impact for each financial transaction device is much higher. Other constraints for electronic financial transactions equipment include security and the associated security certification, which influence both cycle time and cost. Furthermore, security implementation for a point-of-sale (POS) terminal affects both the hardware and software. (In this context, hardware means everything down to the processor supporting all tamper-resistance mechanisms.)

Each new smartphone family involves a new application processor generation, such as the evolution from an ARM11 to an ARM® Cortex-A15 core processor, or migrating from a single core to a dual core processor. In addition to processor advancements, a video decoder or graphics accelerator could be replaced. To facilitate these improvements in design, the semiconductor industry will continue to develop powerful application processors to meet market demand. This is because the size of the cell phone market is big enough to justify the huge investments required for the development of a new high-end microcontroller. These investments include core license costs, mask sets in aggressive nodes technology, and analog blocks development, just to name a few.

Today, the most prevalent architecture trend for POS design is a single-chip secure microcontroller. Such microcontrollers are at the heart of the payment terminal: they embed the processor core, run the operating system, and handle the display and communication functions. They also support the most critical security functions, such as tamper detection, secure key storage with instant key destruction capability, and cryptographic calculation with associated countermeasures.

While the benefit of combining the generic functions of an embedded device with security functions is obvious in terms of BOM and manufacturing costs, it may not be the most appropriate solution to meet stringent development requirements and constraints for high-end devices. While it may be cost-effective to develop a new processor for a family of cell phones due to the potential high number of sales, the size of the financial terminal market does not always justify such developments. Additionally on the software side, migrating a whole operating system and applications family to a new processor represents a significant effort. Security-related software is not available off the shelf and it often has strong hardware dependencies. It also needs to be fully recertified, making the migration effort even more difficult.

In short, the situation for high-end payment-terminal developers can be challenging. They must either create a design using existing secure microcontrollers (and risk creating a design with a soon-to-be-obsolete technology), or they must fund the development of a new microcontroller (bearing the cost of software migration and certification). In the latter case, the economic viability can be highly questionable when developers design a high-end payment terminal that includes numerous value-added features.

So, is there a way to design feature-rich POS equipment at an affordable development cost? Can one take advantage of the efforts made by the cell phone industry by reusing the hardware and software technology developed for this market? The answer is ***yes***, and we will show how to make it happen. Thanks to the smartphone boom, the variety of building blocks for payment terminals, both in hardware and software, is huge. Semiconductor vendors have an extensive range of microcontrollers and system-on-chips (SoCs) available, enabling the design of comprehensive sets of features for a multimedia-embedded device. Not only do the microcontrollers come with an operating system like the Android platform, but developers can also buy off-the-shelf smartphone reference designs. It seems natural for a POS terminal vendor to take advantage of such existing reference designs, which support all generic functions, and then add the security features that are specific to financial terminals. However, adding security functions to an existing system is not trivial if they are not carefully considered at the architecture level.

One of the key challenges for adding security is the display: the PCI PIN Transaction Security (PCI-PTS) standard requires full display control. Without such control, the typical security threat is an untrusted or malicious application that prompts the user for his or her PIN code. Such malware could display a fake "Enter your PIN" message, obtain the user PIN, and send it over to the attacker for fraudulent purposes. To counter this threat, PCI-PTS requires that firmware prevents such a scenario from happening. This requirement does not exist for smartphones, so implementing this control can require in-depth modifications of the operating system and applications. These modifications require a huge amount of design effort and thus reduce the benefit of using a turnkey reference design.

To counter this threat, Maxim's solution is to add a security processor that is capable of taking over the control of the display (**Figure 1**). This security processor is connected to the TFT-bus output of the main processor and the TFT-input bus of the actual panel. It has the full control of the numeric keypad and supports two modes of operations, the **trusted mode** and the **normal mode**.

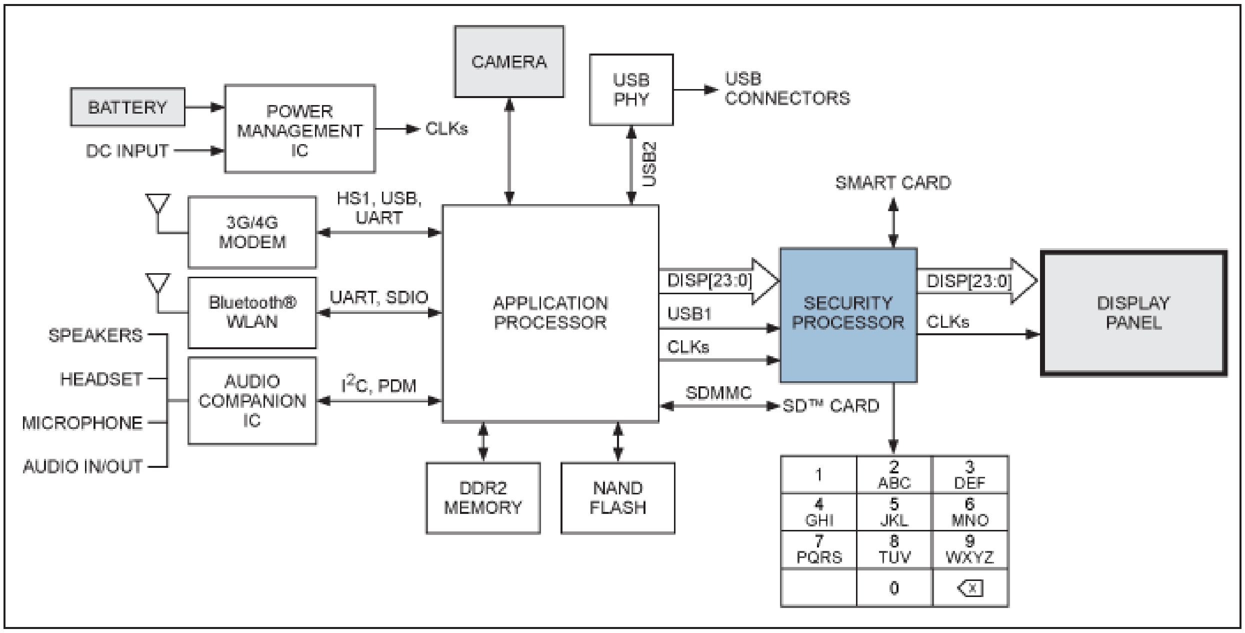

Figure 1. To easily and inexpensively counter security threats, a security processor can be added that is capable of taking over control of the display.

In the **normal mode**, the security processor simply functions as a pass-through system. The keyboard is disabled, and the second processor releases the data on the TFT bus from the main processor flow to the TFT panel. Even if an unauthorized application attempts to display a fake PIN prompt, this has no effect because the keyboard has been disabled. The unauthorized application would never receive any data from the keypad.

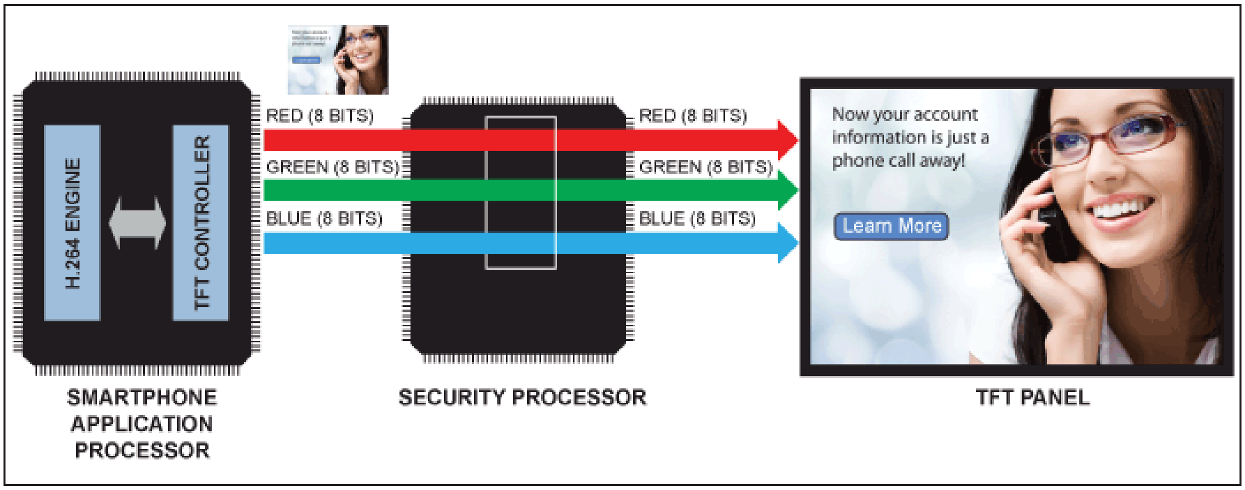

Figure 2. In the normal mode, the security processor acts as a pass-through device.

In the **trusted mode**, the security processor takes full control of the TFT bus and the panel only displays authenticated images, like digital signature verification. Data sent on the TFT bus by the main processor would never be displayed, as the TFT panel input bus is physically disconnected from the main processor TFT output bus. In this mode, the numeric keypad is enabled, so a user can enter its PIN code when prompted.

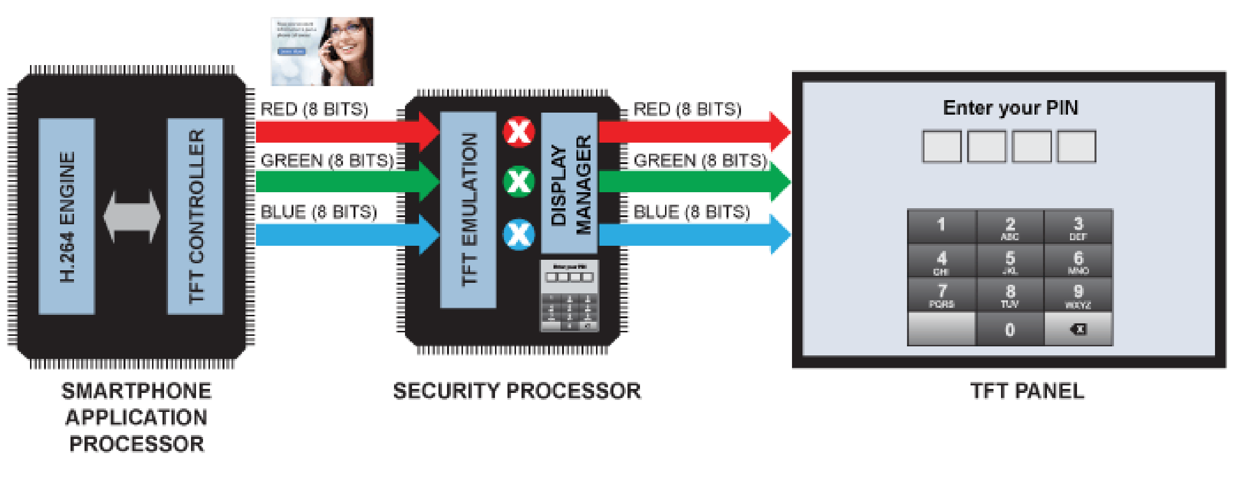

Figure 3. In the trusted mode, the security processor takes control of the panel.

The existence of these two modes is a huge benefit to the equipment's functionality. In the normal mode, the payment terminal behaves almost like a smartphone. It can, for instance, display a video using its original media player without modifying the hardware or software from the smartphone reference design. Also in this pass-through mode, any resolution, color depth, or frame rate can be used. In the trusted mode, the payment terminal is used for standard financial transaction. This functionality is fully embedded in the second processor and does not require any modification to the operating system or applications inherited from the smartphone. Security is truly added to the system by the second processor.

This design also improves the rate of evolution of a POS terminal family. Developing a family of POS terminals with enhanced multimedia features requires a new multimedia processor and the migration of the software to this new controller. If the POS equipment were built around a single microcontroller with embedded security, moving to the next generation would mean investing in the development of a new processor and bearing the cost of a software migration and full recertification. With the approach of a secondary processor, development is much easier: One can start from a smartphone reference design that features the latest multimedia innovations and add the security processor with the same embedded firmware of the previous generation. As the security is not modified from previous generation, the certification is much easier, faster, and less expensive. Using this approach ensures that the end product has all of the state-of-the art multimedia features users could expect.

This strategy does not signify the end of the single-processor architecture for POS equipment. The approach presented here offers the fastest time to market and lowest development costs for very high-end devices, where POS vendors want to follow the feature-rich smartphone trend. For low- and medium-range devices in which the software is less complex (and fewer multimedia features are expected) or when the product cycle is shorter, the single-processor approach with embedded security is still valid.

Maxim is a well-recognized solutions provider for the electronic payment industry. Our comprehensive range of secure microcontrollers enables cost-effective payment terminals design. With Maxim's secure ICs, OEMs can reduce time to market, thanks to our extensive software offers and precertifications. The MAX32590 (JIBE) secure ARM9™-based microcontroller embeds all security mechanisms needed to ensure an easy PCI-PTS 3.1 certification. To enhance security, the MAX32590 includes advanced crypto blocks with state-of-the-art countermeasures, tamper detection mechanisms, and secure storage with advanced wipe mechanisms. The battery-backed area consumption of the MAX32590 is one of the lowest in the market, making it the best option for mobile and portable POS designs. A version will feature the innovative trusted display-control capability described in this article.

References

1. Epstein, Zach. "IMS: Annual smartphone sales to reach 1 billion units by 2016; Apple, Samsung winners so far." BGR, July 24, 2011. http://www.bgr.com/2011/07/27/ims-annual-smartphone-sales-to-reach-1-billion-units-by-2016-apple-samsung-winners-so-far/.%20.

Android is a registered trademark of Google Inc.
ARM is a registered trademark and registered service mark of ARM Limited.
ARM9 is a trademark of ARM Limited.
The Bluetooth word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Maxim is under license.
Wi-Fi is a registered certification mark of Wi-Fi Alliance Corporation.

Related Parts	
MAX32590	DeepCover Secure Microcontroller with ARM926EJ-S 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 5328: http://www.maximintegrated.com/an5328
APPLICATION NOTE 5328, AN5328, AN 5328, APP5328, Appnote5328, Appnote 5328

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