WHITE PAPER

TEXAS INSTRUMENTS

M-Shield™ Mobile Security Technology: making wireless secure

Jerome Azema
Distinquished Member of Technical Staff
WTBU Chief Technology Office - Security
Texas Instruments

Gilles Fayad
Worldwide Strategic Marketing Manager,
Mobile Platform Security and Emerging Applications,
Wireless Terminal Business Unit
Texas Instruments

Introduction

As mobile handsets become increasingly complex, connected and ubiquitous, the need for security on the handset has become essential. Further, the convergence between the mobile device and Internet through 3G and Wi-Fi dramatically increases the potential security threats on handsets.

The vast majority of current phone security solutions are software-based, which are inherently more vulnerable to hacking, viruses and other malicious attacks than hardware solutions.

Operators have traditionally wanted to protect their phone assets and make sure that the handset performs only in the ways expected on their network. This demand has led to protection mechanisms that OEMs have integrated into their handsets, complemented by other OEM-implemented secure mechanisms to further protect handsets from cloning and unwanted modifications.

OEMs have now extended this hardware-based security foundation to begin addressing security requirements of applications and services running on their platforms, such as content DRM and service access protection.

Content providers such as film, music and game publishers – who feed these applications with content – are largely concerned with protecting their creative assets, which end users are downloading. Service providers such as music portals, television broadcasters and financial institutions also want to protect and control access to the services that they provide.

Texas Instruments' M-Shield™ mobile security technology is a system-level security solution, tightly interleaving hardware and software components, that delivers the highest level of security available today while meeting the varied needs of all stakeholders in this value chain including operators, OEMs, content providers and end users.

End users are increasingly accessing advanced services and applications on their handsets, resulting in an increase in transactions and greater storage of valuable financial, personal and sensitive information on the handset. The whole value chain relies on the confidence and trust that the end user has in the handset, application and services provided.

The case for security on mobile handsets

To support the widespread adoption of new services and to address the convergence between the mobile world and the Internet increased levels of security in handsets are essential.

Theft and fraud are a constant problem in the mobile market today. Currently, IMEI/SIMLock features on handsets have been circumvented.

Handsets today are a long way from the basic communication devices of the past; they have become "lifestyle" devices that include multimedia players, cameras, location devices, portable office capabilities and e-Wallet functionality. They help us perform our daily working tasks, entertain us, capture the memories we cherish and facilitate routine transactions. As a result, a wealth of valuable data and information accumulates in our phone's memories and needs to be protected.

Multimedia-feature phones today often carry MP3 audio players, video players and mobile TV applications. Some also boast console-quality 3-D gaming platforms. All of this functionality requires digital rights management (DRM) or control access (CA) services to protect high-value content. The DRM and CA schemes are often associated with content management and protection models, such as Content Management License Administrator (CMLA) or Content Protection for Recordable Media (CPRM), that favor secure, hardware-strengthened content protection. They are also often associated with penalty clauses to further motivate OEMs to adopt strong protection schemes.

Connectivity-enabled phones feature access to the Internet and networking through multiple access technologies such as 3G or Wi-Fi, as well as personal communication means such as *Bluetooth*® and Near Field Communication (NFC). Among these, enterprise-type

phones that enable push e-mail access and office applications have proved extremely popular. They give users a "work anywhere" ability that requires a secure link to their workplace applications through virtual private networking (VPN), secure storage of their data and remote management of the phone by the IT department. Company IT departments are often wary of enabling connectivity access to their networks, fearing that the handsets could carry malware and create attacks from within the network when used on company premises.

These enterprise-type handsets are generally built on high-level operating systems (HLOSs) that provide an open environment to which users can add applications at any time, often with little concern as to the impact on the stability and security of the handset. OEMs want to take advantage of HLOSs but still be in control of what software can run on the phone. By providing the right security, OEMs will be able to help prevent the execution of unauthorized software on the phone, or disable the rollback of software to a previous, less secure version.

Consumers are increasingly using their handsets to access the Internet and perform the same personal and financial transactions as they do from their PCs today. These transactions require SSL/TLS Internet secure protocols as well as a higher level of security for storing personal data on handsets such as credentials, credit card numbers and other personal information. Sensitive information could be exposed in case of loss, theft or through a variety of means, including malware.

Additionally, financial-oriented transactions are emerging, including ticketing and proximity or remote payment functionalities. In some cities you can instantly purchase transportation or movie tickets or pay for a small purchase in a retail outlet by waving your handset next to a point of sales (PoS) device, just as you would with a contactless payment card. These transactions are typically capped at a specific purchase limit; higher levels of security are needed for payments above a certain sum. In some economical models, the handset itself becomes the point of sale, requiring even further degrees of protection.

As described above, hardware-based security measures are becoming an inherent requirement of mobile applications and services for all segments of the mobile market. As the applications and services are deployed, liability models appear to reinforce the need for hardware-based security. Confidentiality and trust are paramount to the adoption and growth in the handset market and mobile services. The wide variety and sources of attacks require a robust hardware- and software-integrated system solution, such as Texas Instruments' M-Shield mobile security technology.

Current security standards

Several security standards from different groups are currently in the market, including the Open Mobile Terminal Platform (OMTP), Trusted Computing Group (TCG), Open Mobile Alliance (OMA), and Third Generation Partnership Project (3GPP). All of these groups have formalized security standards that require hardware-strengthened security to more fully address the security needs of the mobile market today and in the future. Operators, OEMs, and silicon manufacturers have agreed on the profiles, and they have already been endorsed by chipset manufacturers and security solution providers. Operators are already requiring OEMs to conform to these standards.

The OMTP Basic Trusted Environment (TR0) hardware security requirements include:

- Unique 128-bit hardware key
- Hardware-based protection of:
  - IMEI
  - SIMLock
  - ME personalization
  - Secure flash update
  - DRM assets
  - Debugging port

Figure 1: *TI's M-Shield mobile security technology solution complies with the OMTP Basic Trusted Environment standard*

Texas Instruments' M-Shield mobile security technology solution provides one of the highest levels of terminal and content security in the industry. Unlike current software-only security solutions, M-Shield mobile security technology is a system-level approach that intimately interleaves optimized hardware and software to provide the highest level of security available.

M-Shield mobile security technology is a flexible and scalable security solution that can be personalized to multiple platforms. This allows OEMs to quickly design robust software- and hardware-based secure devices. M-Shield mobile security technology sets the benchmark for the level of security required to provide wireless content protection, access control and financial transactions.

Key benefits of M-Shield mobile security technology

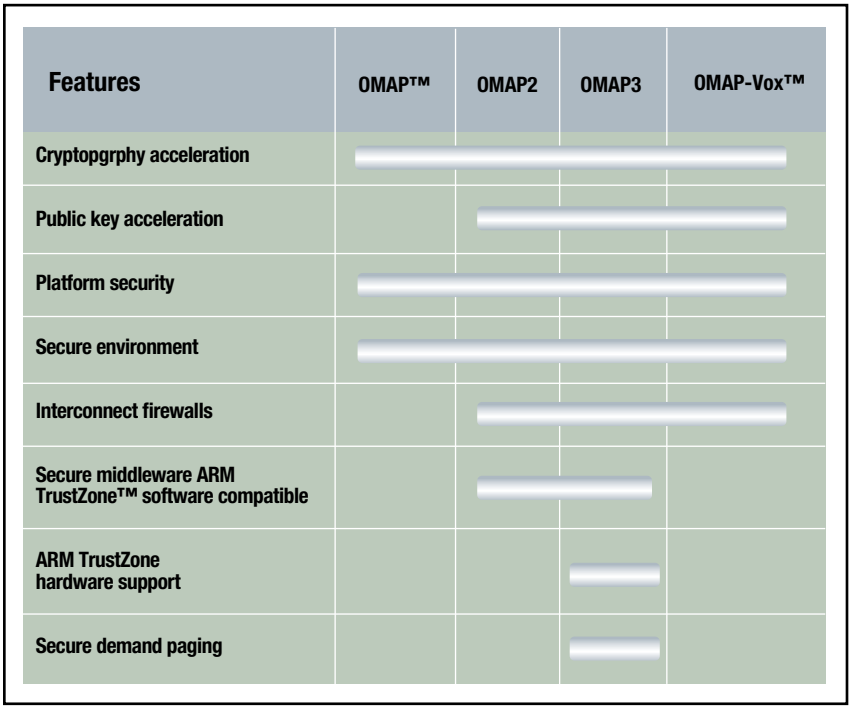
- Highly robust security solution including a complete security infrastructure with on-chip cryptographic keys, secure execution environment, secure storage, secure chip-interconnects and other features
- Standard APIs (TrustZone) that enable interoperability and faster development and streamlining of security-based applications
- Tampering detection triggers effective protection actions
- Flexible security framework that includes a secure middleware component to support third-party middleware software and applications
- High-performance, hardware-based cryptographic accelerators that reduce latencies and deliver a compelling user experience
- Low power consumption maintains extended battery life

Figure 2: *TI's M-Shield mobile security technology offers key benefits to ensure the highest level of security*

Security and the OMAP platform

M-Shield technology is the key security element of TI's OMAP™ platform and OMAP-Vox™ scalable wireless solution. The OMAP platform provides a family of high-performance, low-power-consumption application processors. With an open, flexible architecture, the OMAP platform is driving innovative solutions across the wireless industry.

OMAP-Vox solutions are built on the industry-leading OMAP architecture and integrate the modem and application processing into the same device. OMAP-Vox solutions are optimized to efficiently run a dynamic mixture of applications and communications functions on the same hardware. Complete



M-Shield™ Technology

M-Shield mobile security system solution infrastructure

OMAP-Vox solutions include the analog components, power management and RF devices. M-Shield mobile security technology provides the infrastructure needed to support platform-level security for the mobile device itself, as well as any high-value content transmitted or stored on the device. Safe execution of sensitive applications and secure storage of important data is enabled by a hardware-enforced secure environment. For example, secure on-chip keys (E-Fuse) are OEM-specific, one-time-programmable keys accessible only from inside the secure environment for authentication and encryption.

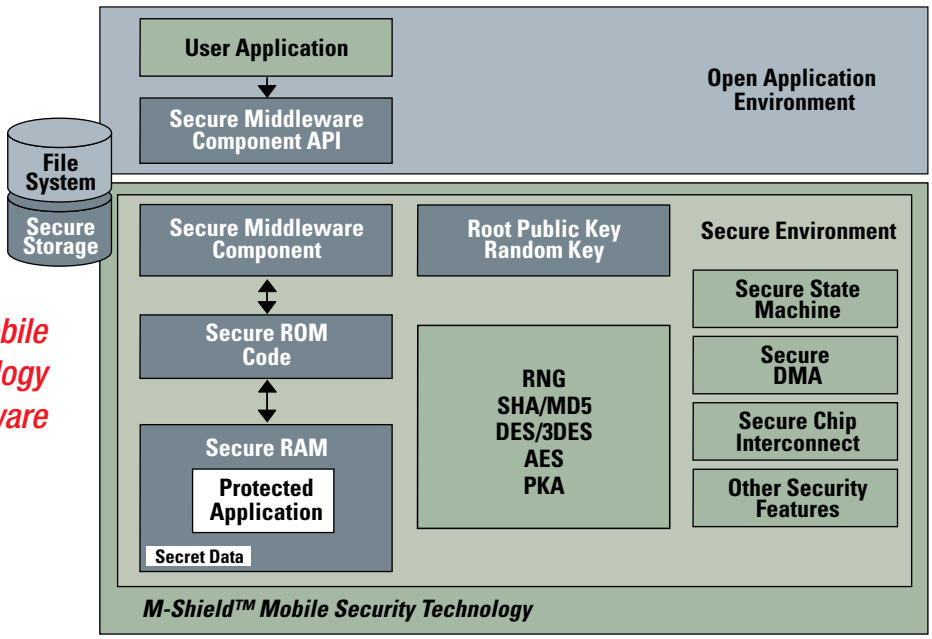
M-Shield mobile security technology offers the industry's leading hardware-based secure environment, embedding a secure state machine (SSM) as well as secure ROM and RAM. The SSM applies and guarantees the system's security policy rules while entering, executing and exiting from the secure environment. Also critical to the overall protection offered by M-Shield mobile security technology is the elimination of the vulnerability of chip interconnects and DMA transfers. TI's M-Shield mobile security technology provides the capability of the secure environment to qualify DMA transfers as secure to protect the confidentiality of sensitive high-value data (such as DRM-protected content) during their processing and transfer throughout the platform.

To further ensure protection against attacks, a secure chip-interconnect allows peripherals and memories access only by the secure environment and/or by secure DMA channels so that the confidentiality of sensitive information is guaranteed through the entire data path, from origin to destination.

Examples of peripherals and memories of the device with controlled secure access include:

- MMI peripherals such as keyboards, LCDs, cameras, fingerprint sensors
- Smart card physical interface
- Cryptographic accelerators
- Serial interfaces involved in multimedia content rendering
- Internal memories
- External flashes and SDRAMs

M-Shield mobile security technology software



Provides hardware and software system level security solution

TI's M-Shield mobile security technology includes a public-key infrastructure that provides a secure means to validate the authenticity and integrity of various software on the platform before execution. The M-Shield mobile security technology solution provides a state-of-the-art hardware-based AES and public-key accelerator (PKA), as well as DES/3DES, SHA and MD5 hardware accelerators.

M-Shield mobile security technology hardware accelerators enhance the user experience by authentication and fast content decryption and integrity checking.

The strength M-Shield mobile security technology solution infrastructure provides reduces the unauthorized use of handsets and fraud while enabling the deployment of value-added secure services.

The M-Shield mobile security technology solution infrastructure provides the highest level of security to reduce the unauthorized use of handsets and fraud while enabling the deployment of value-added secure services.

To complement the M-Shield mobile security technology's hardware-based system-level solution, TI developed a security middleware component that includes a security framework and TrustZone standard-based APIs. This security middleware component enables interoperability, faster development and streamlining of security-based applications.

The secure software environment is also responsible for interfacing the cryptography engine to higher levels of the system, such as the operating system, industry-standard security protocols and interfaces (OMA DRM, WM-DRM, SSL, TLS, IPSec, etc.). With a wide range of TI partners, time to market and ROI can be improved with third-party security applications.

Conclusion

For a high-value services deployment to be successful, end users, content providers, OEMs and service providers must be confident that the handset offers the right level of security. As the value and complexity of applications and high-value content increases, their protection becomes essential to conversely protect the large investments made in them.

For more information

www.ti.com/m-shield