Securing the Mobile World

We are living in a fascinating era in which mobility and convergence between different networks, devices and applications play crucial roles. Over the last few years the performance of mobile communication devices has improved significantly, and these devices have an ever increasing number of features and applications such as creating and managing multimedia, playing games, reading and responding to e-mails, word processing and running business applications. These capabilities are often deployed using the wireless Internet.

The boom of new service providers and the need to send, receive, store and handle sensitive data with mobile devices sets new challenges for both professional users and consumers. Although criminal online activity targeting smart handhelds is currently rather limited, it is justified to introduce securing solutions to the market proactively. The rapidly growing importance of mobile devices requires higher levels of security and assurance.

Standardizing Security

After significant and industry-wide effort, the Trusted Computing Group (TCG) is introducing an open security specification called Mobile Trusted Module (MTM) Specification for mobile devices to the market. The MTM represents a strong security solution for enhanced user privacy and reduced risk of handset theft than is currently available. Moreover, it enables the development of advanced applications and services within the mobile industry environment.

MTM is an open specification for common TCG security building block functions which can be used in a full platform security solution. A phone typically contains multiple MTMs, all of which provide similar functionality to existing TPMs and some of which have additional functionality to boot parts of a phone into a preset state. The MTM has much in common with the current TCG specification for Trusted Platform Modules (TPM) for personal computers. However, it also provides functions which have been developed specifically for mobile devices. Some adaptations are a reponse to restrictions inherent in today's phone technologies. MTMs with just these adaptions are called Mobile Local-owner Trusted Modules (MLTMs), since they merely support usages similar to those of existing TPMs (controlled by an entity with physical access to the platform). Additional adaptions enable parts of phones (not the entire phone) to boot into preset states. These MTMs are called Mobile Remote-owner Trusted Modules (MRTMs), since they enable remote entities (such as the phone manufacturer and the ceullar network provider) to preset the operation of some parts of the phone (such as access to the IMEI and the cellular network). In future specifications, the Mobile Phone Working Group (MPWG) will define a new root of trust that will use MRTMs.

The MTM is designed to extend security and interoperate with existing mobile device components such as SIM, USIM, and UICC cards. In addition, the TCG Mobile Phone Work Group has taken into consideration the security related work which has been done by industry groups such as the OMA, 3GPP, MIPI, OMTP, and others to make sure that the MTM specifications will support and extend security for these other specifications. Thus, the Mobile Trusted Module Specification and future mobile platform specifcations will complement and bring added value to the existing mobile security standards

and are inended to allow multiple trusted devices and components to work together and share the same security infrastructures.

The Characteristics of Mobile Trusted Module

As integration and interoperability have taken remarkable steps ahead over the past years and the field is also charged with ambitious expectations for future, MTM is designed to support a multi-stakeholder phone environment. A stakeholder is an entity which is authorized to have a presence in the phone and which needs the ability to control and protect their individual interests in the phone. Mobile device stakeholders include the user/owner, the network service provider, the device manufacturer, and potentially others such as enterprises and third parties. To that end, the MTM has been designed to enable a trusted and shared environment that is characteristic of mobile devices. A device manufacture and network service provider would typically use a MRTM, while the user would typically use a MLTM.

The aim has been to develop safer mobile platforms and establish an open industry standard for the increasingly sophisticated mobile phone ecosystem that offers added value to private users, businesses, IT companies and networks. In a nutshell, the Mobile Trusted Module is a verifiable security component that enables a trusted computing framework for mobile devices in the *environment* they are used in.

The MTM, like the TPM, protects keys and other secrets while a platform is switched off and only enables keys (and secrets) to be used by the proper entity when the MTM is securely switched on.
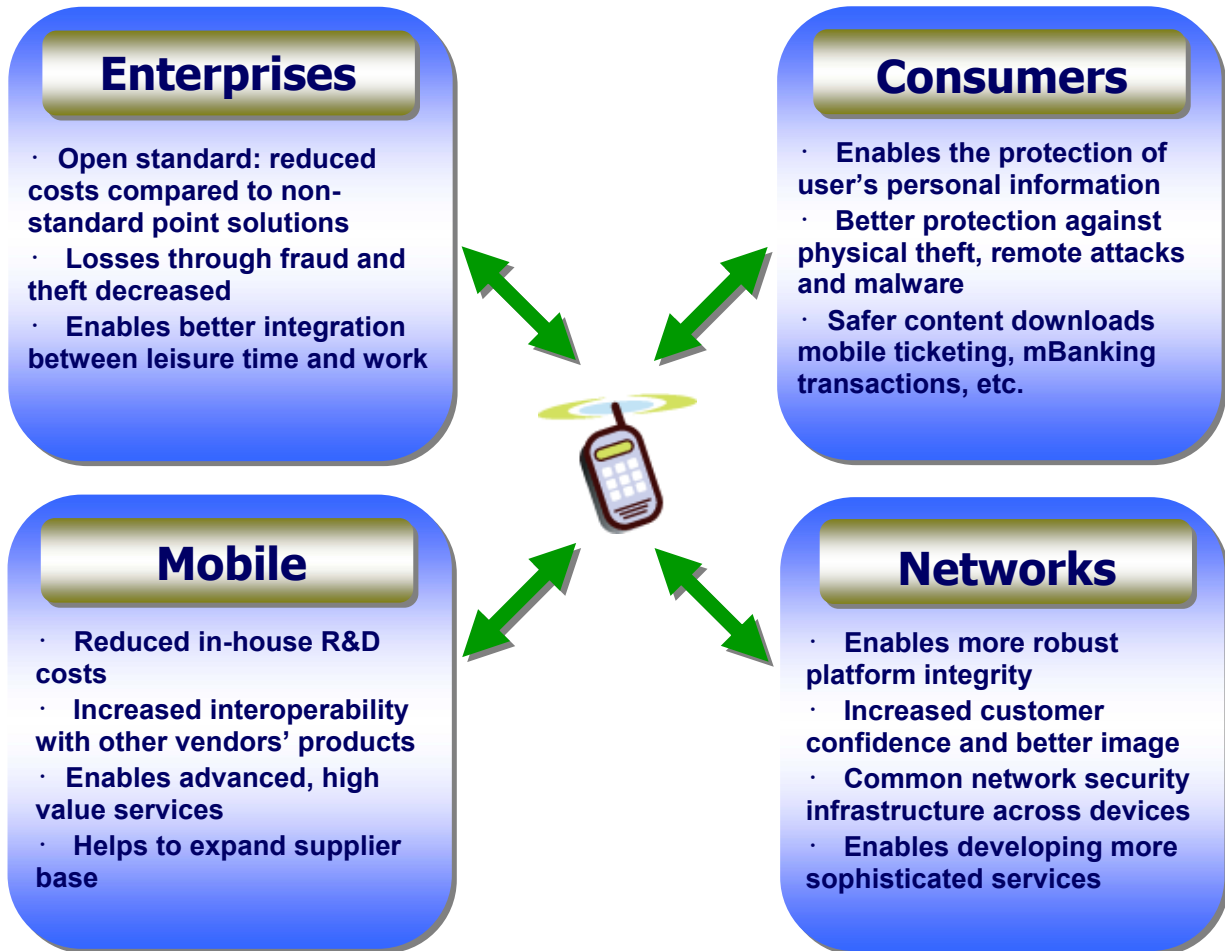
The MTM also:
- Has new commands that enable selected stakeholder applications to boot in a safe environment in the phone, without interfering with the rights of other stakeholders
- Supports techniques to ameliorate the limited availability of protected rewritable non-volatile memory in current phone technologies

The MTM is specifically designed to enable a wide range of implementation choices, from discrete chip solutions to virtualized implementations in System-on-[a]-Chip solutions. Thus it is compatible with existing methods of building phones.

Vendors need to provide software and hardware that provides standard TCG Roots-of-Trust such as the Root-of-Trust-for-Measurement, an additional Root-of-Trust to verify software before loading it, and (optionally) an additional Root-of-Trust for instantiating other Root-of-Trust s. Vendors also need to provide software that can take advantage of the functions provided by TCG technology. This may include adaptation and further development of operating systems. The overall reference architecture will be described in a future companion specification whose development is already well advanced by the TCG.

Mobile Trusted Module – Supporting Multiple Stakeholders

Enterprises

· Open standard: reduced costs compared to non-standard point solutions
· Losses through fraud and theft decreased
· Enables better integration between leisure time and work

Consumers

· Enables the protection of user's personal information
· Better protection against physical theft, remote attacks and malware
· Safer content downloads mobile ticketing, mBanking transactions, etc.

Mobile

· Reduced in-house R&D costs
· Increased interoperability with other vendors' products
· Enables advanced, high value services
· Helps to expand supplier base

Networks

· Enables more robust platform integrity
· Increased customer confidence and better image
· Common network security infrastructure across devices
· Enables developing more sophisticated services

The Multi-stakeholder security architecture ensures long-term development and offers added value that takes the needs of various parties into account.

What's Ahead for Mobile Trusted Module?

Like all TCG specifications, the released version of the Mobile Trusted Module Specification will be available on the organization's website, free of charge. While we are not able to forecast specific product plans, generally products follow specifications by six to eighteen months, depending on product development cycles.

In addition to the MTM Specification, the TCG Mobile Phone Work Group is developing a broader systems reference architecture which incorporates the MTM as a basic security building block and defines a more comprehensive platform security model for handset manufacturers, network operators

and software developers to integrate and take advantage of the added security provided by the MTM. The group anticipates publishing these additional specifications in calendar year 2007.

TCG's mobile phone work group, whose members include Agere Systems, AMD, ARM, Atmel, Authentec, Broadcom, Certicom Corporation, CESG, Ericsson, ETRI, France Telecom, Freescale, Fujitsu Limited, Fujitsu Siemens Computers, Gemalto, Giesecke & Devrient, Hewlett Packard, Hitachi, IBM, Industrial Technology Research Institute, Infineon, Intel, InterDigital Communications, Lenovo, Lexar Media, M-Systems Flash Disk Pioneers, Microsoft, Motorola, Nokia, Nortel, NTRU Cryptosystems, Philips, Renesas Technology, Ricoh Company, SafeNet, Sandia National Laboratories, Seagate Technology, Siemens AG, Signacert, Sinosun, Sony, STMicroelectronics, Sun Microsystems, Symantec, Symbian Ltd., Toshiba, Utimaco Safeware AG, VeriSign, Vodafone, Wave Systems and Winbond have been working to identify security threats, standardized approaches to them, and implementation of Trusted Computing concepts. These companies have also participated and provided their experience in the Mobile Trusted Module Specifcation development process.

FOR MORE INFORMATION, PLEASE CONTACT:

Trusted Computing Group Administration
3855 SW 153rd Drive
Beaverton, OR 97006
E-mail: admin@trustedcomputinggroup.org
Phone: (503) 619-0562, Fax: (503) 297-1090