

Secure electronic transactions—The mobile phone evolution continues

Susanna Friis-Hansen and Bengt Stavenow

Ericsson holds firm to the idea that future mobile phones will be equipped with a single digital ID based on an open, globally accepted standard. The phone will be used for a multitude of trust-based services including e-commerce and secure access to e-mail clients, intranets, and even physical access to property and premises.

In April 2000, Ericsson, Motorola and Nokia jointly established the MeT initiative. The mission of the initiative is to define how certain core technologies should be used in mobile phones to enable electronic transactions. To facilitate acceptance of all parties involved, and applicability in all relevant markets, the strategy for MeT has been to base its framework on existing standards, and to design it to be independent of underlying system standards.

The authors give an introduction to secure electronic transactions, explain the role of the handset manufacturer, and describe MeT and the enabling technologies of the initiative.

Introduction to secure electronic transactions

Being small, handy and increasingly utile, the mobile phone is the central or core device of a mobile society. The addition of novel applications and capabilities make it even more personal and trusted, and thus a regular part of everyday life.

Mobile phones are becoming commonplace products. The number of mobile phone subscribers worldwide is expected to reach 1 billion by 2002. And a significant share of these users will soon be equipped with Mobile Internet-enabled terminals. In fact, by 2003, this group is expected to outnumber users of the fixed-line Internet. Consequently, consumers will have access to

content and services at any time and from virtually any geographical location.

At present, the main use of mobile communications is still voice-related service, but several indicators show that this is changing. Larger displays, packet-data and third-generation networks, Bluetooth, and recent releases of the wireless application protocol (WAP)—which offers adequate security for a wide spectrum of applications thanks to more expressive markup language elements in WAP 2.0—are combining to give good user experience of data-centric services. In many markets, where users are becoming experienced and are interested in finding new ways of using their mobile phones, the stage is set for a successful roll-out of data-centric transaction-based services, such as payment services and ticketing. The mobile phone is thus becoming a personal trusted device (PTD) that is increasingly capable of handling transaction-based functions in the physical and online worlds.

Transaction-based services have caught the interest of powerful stakeholders who are eyeing expanded business opportunities. Operators, for example, are active in the mobile-transactions arena, and see big opportunities in expanding their businesses to become a partner higher up the value chain.

Typical transaction-based services include supporting infrastructure services throughout the various stages of the service life-cycle, such as the issuing of WAP identity modules (WIM), certificate authority (CA) services, and payment-clearing services.

Banks, which are the traditional strong players in the financial sector, are determined to maintain their position by offering financial services in the mobile environment. Examples of services are stock trading, the transfer of funds between accounts, and payment services. Certain progressive banks are already involved in limited trials, and the financial sector generally expects the market for mobile financial services to take off in 2002. Obviously, trust is a key issue. Traditionally, the financial sector has not trusted anyone but itself. Therefore, single-application security solutions, such as secure electronic transactions (SET) and Europay, VISA and Mastercard (EMV), were developed for use in the fixed Internet environment and for point-of-sale terminals. Unfortunately, even though consumers expect to have global access to services, SET and EMV have thus far failed to

BOX A, ABBREVIATIONS

CA	Certificate authority
CUE	Consistent user experience
EMV	Europay, VISA and Mastercard
J2ME	Java 2 platform, micro-edition
MeT	Mobile electronic transactions
PIN	Personal identification number
PKI	Public key infrastructure
PTD	Personal trusted device
SE	Security element
SET	Secure electronic transactions
SIM	Subscriber identity module
SWIM	WIM on SIM
TLS	Transport layer security
WAP	Wireless application protocol
WIM	WAP identity module
WML	Wireless markup language
wPKI	Wireless PKI
WTLS	Wireless TLS

take into consideration geographical differences and the limitations of the mobile phone and the mobile environment. In general, the financial sector, which is wary of operator-driven activities, has stated that regardless of the technical solution employed, operator independence is an absolute must. It sees itself as the obvious supplier of the security infrastructure needed for financial services and wants to have as little involvement from operators as possible.

Apart from the companies involved in e-commerce-related applications, numerous security companies offer their own security infrastructure (servers and clients) for e-mail, secure access to, say, a corporate intranet, and physical access to buildings.

This is still very much an emerging market fraught with numerous contending technologies and devices, and a lack of widely accepted standards and global solutions. This fragmentation is serious and potentially threatening to market development. Because content and service providers must take into consideration all possible products that might be used to access services, the development process will be slow and tedious. What is even more serious, however, is that the user experience, which is the basis for creating consumer trust, is inconsistent. If consumers are to turn to the capabilities of their mobile phones for making payments, accessing e-mail clients, and for gaming and ticketing services, then the mobile phone must be easier and more convenient to use than credit cards or some other secure-access device that can be carried in the wallet. In addition, consumers must feel that the services can be trusted and that their integrity is being protected. Otherwise, consumer behavior will not change.

As a whole, the wireless application protocol, its associated WAP security elements, and the consistent user experience (CUE) defined in MeT have been proven to fulfill the requirements of the various stakeholders in multiservice environments. Furthermore, the Mobey Forum has stated its active support of the WAP identity module for remote mobile financial services. Thus we have clear indications that the major players of the financial industry all actively support WAP and its associated security elements as a viable solution for the mobile environment.

Still to be resolved, however, is the issue of how the WAP identity module is to be implemented. For operators, the obvious el-

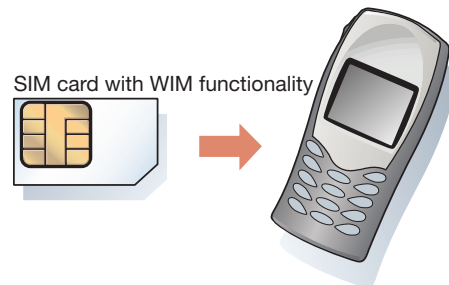


Figure 1
WIM on SIM implementation.

ements of a technical infrastructure show WAP and WIM implemented on the subscriber identity module (SIM). By issuing WIMs, operators can give customers new business opportunities. This in turn strengthens the customer relationship. On the other hand, the financial sector is reluctant to support this kind of implementation, since it takes the issuing process out of their hands and makes them dependent on operators. What is more, the financial sector is afraid that it will lose business opportunities when operators eventually begin offering payment services. Instead, to retain full control of the WAP identity module, the financial sector wants to issue WIM cards that are physically separate from the subscriber identity module—that is, it wants to see a dual-chip implementation.

The role of the handset manufacturer—Ericsson

Ericsson holds firm to the idea that the mobile phone will be equipped with a single digital ID based on an open, globally accepted standard. The phone will be used for

TRADEMARKS

Bluetooth is a trademark owned by Telefonaktiebolaget LM Ericsson, Sweden.

Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

MasterCard is a registered trademark of MasterCard International Incorporated.

MeT is a trademark owned by MeT and its sponsors.

VISA is a registered trademark of Visa International Service Association.

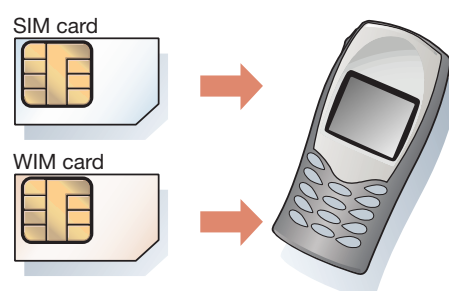


Figure 2
Dual-chip (separate SIM and WIM) implementation.

a multitude of trust-based services including e-commerce and secure access to e-mail clients, intranets, and eventually—when the Bluetooth infrastructure is in place—physical access to buildings. The basis for the digital ID is the WAP identity module. The mobile phone thus becomes the user's personal trusted device and enabler of the mobile society.

Ericsson will play an active role until the market for secure transactions has matured. Apart from implementing the required

technology, to help build the market and create the critical mass of customers and services needed for market take-off, Ericsson is involved in several field trials and demonstrations to give *proof of concept* and to collect feedback. In Hong Kong, for example, all the operators have joined forces to set up a collective certificate authority. The field trial includes content providers, an infrastructure, and users (initially 100). And in the spring of 2001, Ericsson and RSA Security demonstrated secure access to e-mail

BOX B, TERMS AND DEFINITIONS

TERM	DEFINITION
Access PIN	PIN that protects WIM data and authentication keys (called PIN-G in the WIM specification).
Authentication	Verification of identity.
Authentication key	Private key used during authentication.
Authorization by user	Process whereby the user authorizes a transaction to be charged to his account. Involves an application-layer digital signature from the user, and provides proof of commitment.
Brand elements	Name, URL, images, or jingles that relate to a service or service provider.
Certificate database	Storage area in the PTD for service certificates and root certificates.
Consistent user experience	Similar user experience among phones of different makes and types. For example, any Web shopping user experience should be largely similar among MeT-compliant phones. CUE also includes consistency of user experience when using the same core function in different usage scenarios (for example, the user authorization experience should be the same in Web shopping and retail shopping usage scenarios).
Content provider	Provides goods and services to the user by hosting a content server.
Contract	Data object on which the user creates a digital signature when making a commitment (identical to the stringToSign in first realization).
Core functions	Basic functions on which MeT is based: initialization, registration, secure session, authentication and authorization.
Dual-chip	WIM implemented on a SIM-sized smart card separate from the SIM.
Dual-slot	SIM application toolkit-based solution for support of full-sized smart cards, currently supported in Motorola and Sagem phones only.
Initialization	Provides the PTD with one or more public-private key pairs and root certificates.
Issuer	Entity that has issued a service certificate for a key pair in the PTD. Typically a bank or a credit card company. The entity and its supporting infrastructure are used synonymously.
Local environment	MeT-defined environment in which the PTD gains access to content via a local or personal area network.
Personal environment	MeT-defined environment in which the PTD is used with other computational resources in a private (secure) environment.
Personal trusted device	Mobile communications device which can be personalized (through the registration of service certificates) and trusted by the user and service providers that require application-level public key security.
Registration	Provides the PTD with a service certificate that relates to a public-private key pair residing in the PTD.
Remote environment	A MeT-defined environment in which the PTD gains access to content via a public mobile network.
Root certificate	Certificate needed for handshake between server and client to achieve WTLS class 2 (server authentication) or higher.
Secure session	Guarantees confidentiality, data integrity and server authentication.
Security element	Component of the PTD that contains the user's key pairs and root certificates and is responsible for performing encryption and authentication functions.
SE initialization interface	The interface (process) that equips the PTD with key pairs and root certificates.
Service certificate	Certifies that a public-private key pair is valid for a specific service.
Service execution interface	Interface (process) that allows a content server to access MeT functions on the PTD.
Service registration interface	Interface (process) that enters service certificates into the PTD.
SignText	Application-level signature function in WMLScript Crypto Library (a WAP specification).
Sign-up	Process whereby the user subscribes to a service and registers the PTD (for the service).
Signature key	Private key used for creating digital signatures on contracts.
Signature PIN	PIN that protects a signature key (called PIN-NR in the WIM specification).
SWIM	SIM card with WIM application.
Transaction database	Storage area in the PTD for transaction data and secure objects, such as receipts and tickets.
Unblock PIN	PIN that can be used to unblock blocked PINs.
User verification	Process that requires the user to enter a PIN to permit access to a key pair.
WIM	Tamper-resistant device used to perform WTLS and application-level security functions, and to store and process information needed for user identification and authorization functions.
WIM card	WIM implemented on a smart card.
wPKI	PKI optimized for WAP.
WTLS	WAP equivalent of TLS.

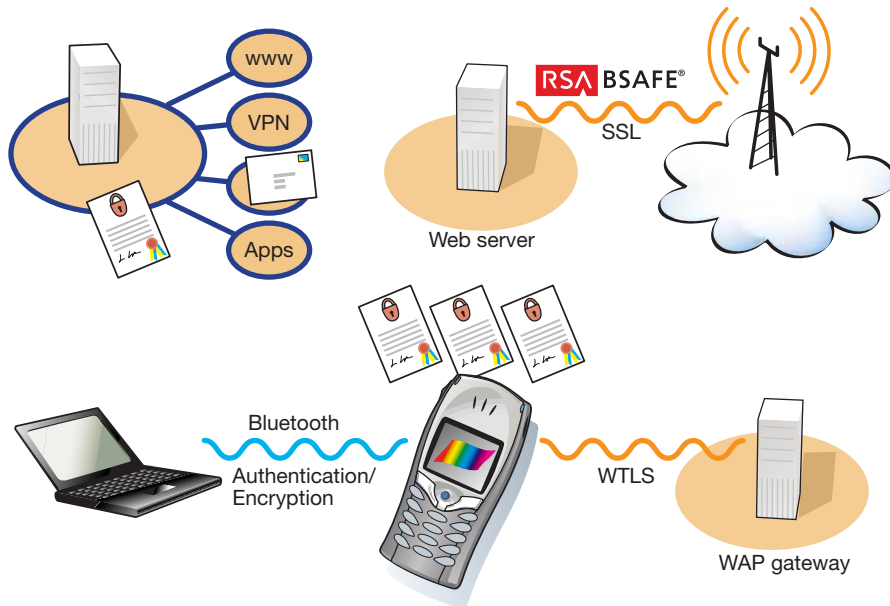


Figure 3
The WIM in a non-commerce application:
secure access to an e-mail client.

clients—a PC was used for accessing services, and a mobile phone served as the authentication device.

Within the EU, activities are underway to regulate mobile e-commerce—for instance, in the eEurope smart card charter and the data protection act. Here, too, Ericsson is playing an active role to ensure that legislation takes into account the abilities and limitations of the mobile phone

Ericsson will also ensure that MeT compliance, including the level of security supported in its entire product portfolio, meets the requirements of the different stakeholders, since secure transactions are expected to be a mainstream application and not a feature exclusively targeted to advanced high-end users.

MeT

As discussed above, mobile phone manufacturers will face certain challenges as the use of mobile phones extends into new areas of application, such as secure transactions. To date, no single standardization body has provided a generic framework for regulating how business-to-consumer mobile electronic transactions (MeT) can be handled securely on mobile phones. To cope with this situation, Ericsson, Motorola and Nokia—the key players in the Mobile Internet market—jointly established the MeT initiative in April 2000. Panasonic, Siemens and Sony

have since joined the initiative as sponsors, making MeT the most significant standardization body for mobile phone-centric electronic transactions. Apart from major handset manufacturers, network operators (France Telecom and Telia), security companies (for example, RSA Security) and the financial sector (including the Mobey Forum and BBVA) are also members of MeT, ensuring broad market and applications support.

To facilitate acceptance of all parties involved, and applicability in all relevant markets, the strategy for MeT has been to base the framework on existing standards, and to design it to be independent of underlying system standards. The core technologies for the MeT framework are

- WAP—the global, open application execution environment for the Mobile Internet;
- WIM—which provides the security elements required for electronic transactions;
- Bluetooth wireless technology—the core technology for local communication with good cost/performance ratio; and
- wPKI—the wireless public key infrastructure is the standard security framework for managing keys and certificates adapted to the wireless environment.

In short, the mission of the MeT initiative is to define how these core technologies will be used in mobile phones to enable elec-

BOX C, WIM IMPLEMENTATIONS

The WAP WIM specification, on which the MeT specifications are heavily dependent, defines the interface between the WAP client and the WIM module. The WAP WIM specification basically includes two parts with complementary objectives:

1. A functional, implementation-independent definition of WIM.
2. An example of WIM implemented as a smart card—based on the ISO7816 series of standards [ISO7816] and, where applicable, the related GSM specification [GSM_SIM].

The specification also clearly states that it has been written to enable alternative implementations based on secure token technology. The most likely implementation in the near future is called WIM on SIM, or SWIM, but other implementations can also be envisaged. For example, the financial sector is afraid of losing business opportunities when operators who own and issue SWIMs start to offer payment services. Consequently, to retain full control of their business, the financial sector proposes that WIMs should be physically separate from SIMs, a proposal referred to as dual-chip.

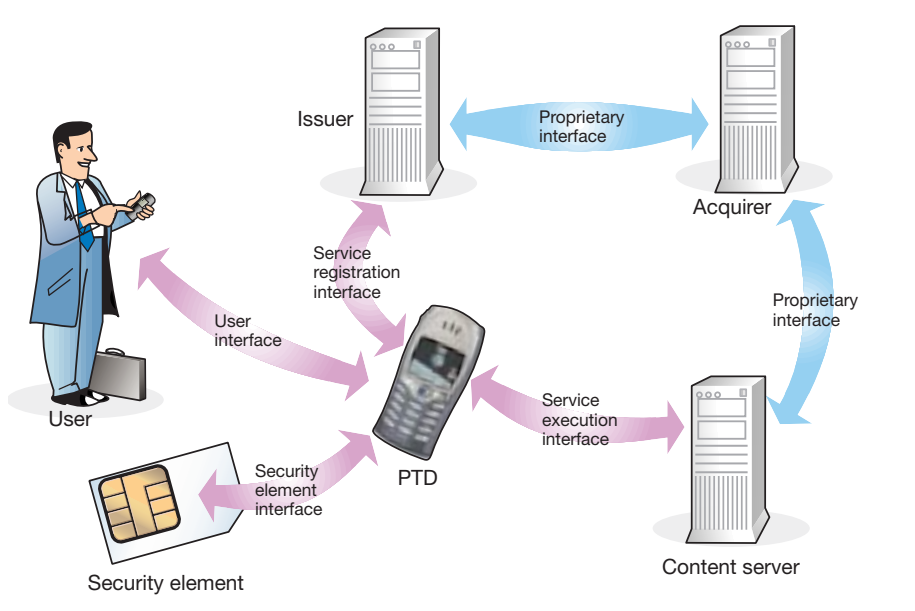


Figure 4
The MeT reference model.

BOX D, CORE MET FUNCTIONS

Five core functions have been defined for the MeT specifications:

Initialization

The mobile phone (PTD) is provided with public-private key pairs that are stored on a SWIM card or on a separate WIM card. The key pairs might also be created in the secure token.

Registration

The PTD is provided with service and root certificates that can be provided on the SWIM or WIM card at the time of initialization, or can be downloaded to the PTD by means of the WPKI framework.

Establishment of secure session

Transport layer security is used to establish a secure session. The technology employed might vary from environment to environment.

Authentication

The client is authenticated using the corresponding service certificate. Use of the certificate is controlled by a related access rule, which requires an access PIN.

Authorization by user

The PTD uses a signature key (different from the private key used for authentication) to create a digital signature. To access the signature key, the user must enter a signature PIN.

electronic transactions. The framework should thus prevent fragmentation and ensure global interoperability. The first comprehensive version of the MeT specifications, published in February 2001, includes

- the core specification, which defines a system reference model (Figure 4), applicable environments, a set of core functions, and security technologies;
- terms of reference;
- a definition of the personal-trusted-device concept;
- a core usage model for account-based payments; and
- usage scenarios, such as for remote banking, retail shopping and WAP shopping.

To complement these specifications, the MeT initiative provides guidelines on a consistent user experience for the entire security framework. A cornerstone of MeT, CUE defines the sequence of interactions in typical transaction phases, such as certificate download, authentication, and the process of entering a digital signature. In addition, CUE defines mechanisms for heightening user awareness of security and branding. The next revision of MeT specifications, due in

early 2002, focuses on ticketing, receipts, the personal environment, and local payments.

To fulfill its strategy and objectives, MeT has established close relationships with other relevant standardization bodies and industry fora. The Mobey Forum, for example, provides the financial industry's view on mobile electronic transactions. The security framework is heavily based on the security technologies specified by the WAP Forum—WTLS, WIM and the WMLScript SignText. Similarly, in Bluetooth standardization efforts, an interest group is working to ensure that Bluetooth technology will be fine-tuned to support MeT usage scenarios in the local environment. And finally, the WAP Forum is addressing the adaptation of the PKI standard to the wireless environment.

Enabling technologies

As mentioned above, the strategy of the MeT initiative is to promote—and if necessary, extend—existing standards and technologies as the foundation for electronic transactions. Basically, three types of key enabler are needed:

- an open application execution environment that can support mobile phones when they
 - subscribe to a service; and
 - access and execute a service for electronic transactions;
- a generic but versatile security toolbox; and
- a range of access technologies that offer cost-effective solutions for the remote, local, and personal environments in which mobile devices are expected to operate.

In addition to embodying these key enablers, the mobile phone should be able to operate as a personal trusted device. That is, besides being a device for mobile telephony, it is also a device with the characteristics required for handling electronic transactions in a secure, trustworthy and consistent way.

Early on, the standardization activities of the WAP Forum were recognized as being key to the MeT initiative. The WAP browser environment, or WAP application environment and associated user agents, can efficiently handle service registration inter-

faces and the service execution interface. Furthermore, the WAP browser technology is expected to be available in virtually all mobile phones by the time the MeT specifications are deployed. This means that service designers have a generic application environment from which they can quickly and easily design, verify and provide new services. In the future, other open application environments, such as Java environments, will also probably be enabled to support electronic transactions. However, this is not presently the case for the Java 2 platform, micro-edition (J2ME)—before it can support electronic transactions, this version of Java must first be extended with class libraries that correspond to the security features found in WAP. This is expected in about two years (2004).

The WAP Forum is also driving activities to standardize other key technologies, such as

- transport layer security (WTLS and TLS)
- a generic security toolbox based on the WAP identity module; and
- wPKI.

Due to constraints in memory and processing power, the task of providing a security framework in a mobile phone is complex. Therefore, the security framework must be applicable to all applications that require security. It must also be applied consistently across all services and applications, so that end-users find it easy to use and can recognize the basic usage scenarios as they move from service to service.

The WAP protocols have been designed to be independent of system standards. As such, they can be run on practically any wireless access technology in the remote environment as well as on technologies for local and personal environments, such as Bluetooth. Enhancements to the Bluetooth and protocol technologies are being considered in relevant standardization groups to better adapt these technologies to the MeT usage scenarios. Examples include shorter discovery times and faster connection set-up in payment scenarios.

Conclusion

Although the market for secure transactions is still immature, there are clear indications that a multiservice mobile society is emerg-

ing. All major handset manufacturers, including Ericsson, have joined forces in order to define how security is to be implemented in the mobile phone and how it is to be used. Local markets around the world are maturing, which means that users are becoming increasingly willing to use their mobile phones for new kinds of services and applications. Banks and operators, currently the two strongest players in the mobile transactions arena, are setting their roadmaps. In mature markets, such as Scandinavia, we will see a roll-out of remote financial services in 2002; other markets will follow in 2003. Services that depend on Bluetooth-enabled infrastructure, such as local payments and physical access to premises, will need another three to four years of deployment.

Ericsson is convinced that future mobile phones will be equipped with unique digital credentials to be used for a multitude of services. The phone is thus becoming a personal trusted device, not only because of technical advances but also because consumers are increasingly willing to use their phones for non-traditional services, such as transaction-based services. Many new technologies and applications (Java, MExE, transaction-based services) will be or already are supported in the current portfolio. All of them demand security. Since the digital ID is essentially a WAP identity module (WIM), and WAP protocols have been designed to be independent of systems standards, the security elements can be used in this broad spectrum of applications.

The obvious placeholder for the WIM is on a card stored in the phone. Built-in solutions strongly discourage consumers from using multiple phones. In Ericsson's current product portfolio, many phones already support the combined WIM on SIM (SWIM). Moreover, beginning in 2002, Ericsson plans to implement this solution throughout its entire product portfolio. SWIM offers the level of security required by the major players, and does not put constraints on design or burden the handset manufacturer with liability. Of course, Ericsson acknowledges the need to grow the market for secure transactions, and is therefore also investigating alternative WIM implementations.

BOX E, STANDARDS BODIES

MeT (www.mobiletransaction.org)

MeT defines a technical framework for secure electronic transactions from a mobile phone, ensuring consistent user experience. Its members include all major handset manufacturers, security companies, the financial sector, and operators.

Mobey Forum (www.mobeyforum.org)

The mission of the Mobey Forum, which is driven by the financial industry, is to encourage the use of mobile technology in financial services, such as payments, and remote banking and stock trading. Its members include BNP Paribas, Ericsson, Nokia, Nordea, and VISA International.

GMCIG (www.gmcig.org)

GMCIG is an open and global organization that develops and submits secure wireless standards to existing standards organizations. Its members include Deutsche Postbank AG, Europay International, Motorola, and NTT DoCoMo.

Radicchio (www.radicchio.org)

Radicchio aims at establishing a common foundation for secure m-commerce by reaching a consensus on important interoperability issues. Its members include Ericsson, Gemplus, Siemens, Sonera Smarttrust, and Mastercard.

WAP ecomeg

WAP ecomeg is a working group of the WAP Forum. The focus of the group is on all issues relating to e-commerce.

BOX F, PRODUCT ROADMAP

By working with standardization and through an aggressive product roadmap, Ericsson has shown its commitment to the MeT initiative.

- With the R320, Ericsson introduced WAP technology with a basic level of security.
- With the R520, T39 and T65, Ericsson's product portfolio enables basic MeT usage scenarios by providing key technologies, such as
 - SWIM (WIM on SIM);
 - root and client certificates through combined initialization and registration;
 - transport layer security through WTLS class 3; and
 - application-level digital signature support (SignText).
- Ericsson's next generation of mobile phones is expected to be fully compliant with MeT—that is, in addition to supporting the features mentioned above, future phones will support wPKI and fulfill MeT requirements for consistent user experience (CUE).