



Using Public Key Cryptography in Mobile Phones

White Paper



Discretix Technologies Ltd.

By Limor Elbaz, VP. Research
Limor.Elbaz@Discretix.com

October 2002

ABSTRACT

As mobile networks expand their bandwidth, mobile phones, as with any other Internet device, become substantially exposed to Internet security vulnerabilities. Public key cryptography is a primary concept in implementing wireless device security. Many papers have been written about public key infrastructure, this paper does not delve into the deeper mechanisms of PKI. Instead, it describes the applicative use of PKI in current and future mobile phone applications, and shows how Discretix CryptoCell™ efficient, lightweight and standard-compliant implementation of cryptographic algorithms, enables wireless devices to become PKI-enabled.

SECURITY THREATS IN THE MOBILE ENVIRONMENT

Being based on the concept of transferring data through intermediate nodes, the very nature of Transmission Control Protocol/Internet Protocol (TCP/IP), the basic communication protocol over the Internet and intranets, makes it possible for an adversary to interfere with communications. Any TCP/IP session may be interfered with in the following ways:

- *Eavesdropping* - the information privacy is compromised without altering the information itself. Eavesdropping may imply that someone has recorded or intercepted sensitive information (e.g. credit card numbers, confidential business negotiations).
- *Tampering* – the information is altered or replaced and then sent on to the recipient (e.g. change of an order or commercial contract transmitted).
- *Impersonation* – the information is passed from or to a person pretending to be someone else (this is called *spoofing*, e.g. by using a false email address or web site), or a person who misrepresents himself (e.g. a site pretends to be a books store, while it really just collects payment without providing the goods...).

3rd generation cellular technology is constantly evolving, supporting broadband, packet-based transmission data, and providing always-on connectivity to phones and other wireless communications. Therefore, all the security threats that we are familiar with in the Internet, invade the cellular wireless networks as well, and translate into risks for commercial transactions, corporate data and personal information.

PUBLIC KEY CRYPTOGRAPHY PROVIDES COUNTERMEASURES

Public-key cryptography is a technique, ingrained in well-known standards, that allows taking precautions, by providing:

- *Encryption* - allows concealing information transmitted between two parties. The sender encrypts the information and then sends it, and the receiver decrypts the information before reading it. The information in transit is unintelligible to an eavesdropper.
- *Integrity (Tamper detection)* - allows the recipient of information to verify that a third party has not altered the information in transit.

- *Authentication* – allows a receiver of information to verify the origin of information.
- *Non-repudiation* – prevents the sender of information from claiming at a later time that he/she never sent the information.

PUBLIC KEY CRYPTOGRAPHY ESSENTIALS

Public-key encryption (also called *asymmetric encryption*) relies on a pair of keys - a *public key* and a *private key* - associated with an entity (a person or computer). These keys are mathematically related, data encrypted with one key can only be decrypted by the other key, however one key cannot be derived from the other key. The public key is distributed, optionally using a digital certificate¹, and the corresponding private key is kept secret. The relation between the keys is used as follows:

- *Public key encryption* - to send encrypted data to someone, the sender encrypts the data with the receiver's public key, and the receiver decrypts it with his/her (corresponding) private key. Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to exchange a symmetric key, which then can be used to encrypt additional data. This approach is frequently used by many security protocols and is called *hybrid encryption*.
- The reverse scheme, sometimes called *private key encryption*, is also useful, being used for digital signatures. A person can digitally sign data by encrypting it with his/her private key. The receiver can use the signer's public key to verify the digital signature. Given that data verified with a public key could have been signed only with the corresponding private key, which is possessed only by its owner, digital signatures provide authentication, non-repudiation and tamper detection. These are the most essential building blocks for electronic commerce and banking.

USAGE OF PUBLIC KEY CRYPTOGRAPHY IN WIRELESS SECURITY

Public key techniques have been adopted in many areas of information technology, including network security, operating systems security, application data security and Digital Rights Management (DRM). Internet standardization bodies, such as the Internet Engineering Task Force (IETF)² are constantly influencing the standardization process of the mobile platforms and specifically the cellular environment. Consequently, cellular-related standards have already adopted PKI as a fundamental element in the construction of security for the near and far future of wireless environment. The following sections provide an overview of public key cryptography use-cases in the cellular environment.

¹ A digital certificate is an electronic identity, constructed of a public key and an identification of the owner of the corresponding public key. Digital certificates are issued, managed and revoked by a Certificate Authority (CA).

² <http://www.ietf.org>

Secure Browsing

Network security protocols are probably the most common use of public key methodologies by wireless devices. The Open Mobile Alliance (OMA, formerly the WAP Forum)³ has specified a Wireless version of the IETF *Transport Layer Security (TLS)* protocol, known as *WTLS*, to secure mobile browsing. WTLS provided for a secure channel between the mobile phone and a WAP gateway, however, did not satisfy the demand for end-to-end security in data networks. A later version of WAP (2.0) adopted the TLS protocol itself within *WAP Transport Layer end-to-end Security* specification. The TLS protocol allows for true end-to-end security while browsing the Internet by:

1. Allowing a web server and a client (in this case – a mobile phone) to authenticate each other and establish an encrypted connection. The authentication is part of the handshake process, where public key cryptography is utilized to provide mutual authentication and shared key agreement.
2. Once the handshake is successfully completed, application data is securely exchanged by means of symmetric key encryption using the shared-key.

Access to Enterprise Networks

One of the greatest promises of 2.5G and 3G wireless networks is enabling mobile devices to access execute corporate applications, such as email, file transfer, CRM and others. This raises the need for a *Virtual Private Network (VPN)* client application that will provide network layer security between the mobile device and the corporate gateway (or the end server). VPN clients may be implemented at different layers, whereas the dominant implementation is within the Internet Protocol (IP) layer, using the IETF *Internet Protocol Security (IPsec)* protocol. IPsec protects the exchanges at the network layer, providing data origin authentication, data confidentiality, replay protection and data integrity. IPsec uses PKI as part of the *Internet Key Exchange (IKE)* protocol, which facilitates automatic key management. IKE handles the exchange of security parameters prior to communication, by the establishment and maintenance of Security Associations. IKE also allows a VPN server to authenticate a mobile device using address independent credentials (user certificates). VPN is already a powerful motive for enterprises to deploy public key infrastructure incorporating the set up of a Certificate Authority (CA) to deploy digital signatures. Once this infrastructure is in place for remote users, it can surely serve remote wireless users as well.

Mobile Payment Authentication

Public key cryptography is considered as a preferred architecture for mobile commerce and banking. The most notable illustration for this is Visa *Three-Domain Secure (3-D Secure™)* specification. Its architecture relies on the issuer's ability to authenticate a remote cardholder by a pre-determined mechanism, where necessary data may be collected during the enrollment process. The *3-D Secure Wireless Authentication Scenarios* specification presents several

³ <http://www.openmobilealliance.org>

authentication methods relevant for the wireless environment, including shared secret, signature and biometrics. The most secure scenario is that of a signature, that relies on public key cryptography.

Local (proximity) transactions are also regarded as a future application of wireless phones. The Mobey⁴ forum has recently adopted the *EMV* protocol⁵ for these transactions, in *Mobey Local Preferred Payment Architecture (Local PPA)* specification.

Access control

A mobile phone with public key cryptography capabilities can also be used as an authentication device for access control systems, based on the challenge-response mechanism, where the phone receives a challenge from a server and generates a response. The mechanism may be based on the use of a symmetric or asymmetric algorithm. Symmetric algorithms require initialization of the phone with a secret, specific to each application, which is often impractical. As opposed to asymmetric algorithms that only require the server to attain the user certificate for signature validation. The Mobile Electronic Transactions (MeT)⁶ group is working on a local authentication protocol called *Personal Transaction Protocol (PTP)* that will allow users to authenticate themselves at retail locations, ticket collection points, workstations, etc. using their cellular phones.

Digital Signatures on Mobile Transactions

Digital signatures make public key cryptography a most practical tool in real-life applications, being the most reliable method for authentication and non-repudiation. As such, digital signatures are expected to become a fundamental element of mobile devices business applications, as they already are being used for signing transactions, taking place in online banking and payment applications. A new concept for mobile transactions is called *actionable alerts*. These are constructed by a service provider sending a message to the mobile user, and the mobile user responding with an alert. A secure version of actionable alerts application, based on digital signatures and encryption, allows the banks to facilitate mobile platforms to secure banking transactions.

Similarly, other procurement transactions may be secured by engaging digital signatures, where the mobile user signs documents such as a contract, NDA, MOU, RFP, bids etc.

⁴ <http://www.mobeyforum.org>

⁵ EMV2000 (<http://www.emvco.com>) consortium is comprised of Europay International S.A., MasterCard International Incorporated, and Visa International Service Association. In December 2000, EMV2000 published the *Integrated Circuit Card (ICC) Specification for Payment Systems*. This specification describes the minimum-security functionality required of integrated circuit cards (ICCs) and terminals to ensure correct operation and interoperability of payment systems. This functionality is based on public key operations. For example, offline (static and dynamic) data authentication uses digital signatures.

⁶ <http://www.mobiletransaction.org>

Messaging

Public key cryptography can also be used to secure other kinds of mobile messaging, such as SMS messages or wireless email applications using *S/MIME* (*Secure/Multipurpose Internet Mail Extensions*) - a specification for secure electronic mail messages in MIME format.

Content Authentication

Code signing is an essential technology for mobile devices that enable application download over the air, such as Java applets. It is necessary, for such devices, to have the means to assure the safety of the downloaded code. The originator or the provider of the code may provide such assurance by digitally signing the code, via an XML digital signature, Java API or by other interfaces. The phone holds a trusted copy of the signer's public key, for verifying the code's signature before using it. Code signing, does not in itself, certify the safety of the code, but it assures that the code was not originated or modified by illegal parties.

Digital ID

A digital ID identifies its holder for multiple purposes, such as driver's license, healthcare, insurance policy etc. Digital IDs are implemented in the form of user credentials and associated certificates. The digital IDs are created and digitally signed by the relevant authority, according to their purpose. When used in wireless devices, digital IDs reside on the device, and can also be transferred (for example, in case of replacing the wireless device), either using a detachable card as intermediate medium, or over the air.

Digital Rights Management (DRM)

Multimedia content (music, video, e-books etc) is stored, distributed and consumed by digital means, forming the need for digital rights management to protect the owners' legal rights.

One example for an end-to-end protocol for the distribution of music data from the host, through the playing device (a mobile phone), to the storage card, is defined in the *Universal Distribution with Access Control – Media Base (UDAC-MB)* specification, and adopted by Keitaide-Music⁷ consortium. UDAC-MB uses the encryption of content-specific license keys, for distributing media, to be read by compliant devices. UDAC-MB uses public key cryptography, to encrypt licenses (including keys for the encrypted media), which are passed from the license server to the playing device. Public key cryptography allows for passing keys securely, where symmetric encryption is not practical, as it would require all the license servers and all the playing devices to share secret keys.

The MultiMediaCard Association (MMCA)⁸ promotes the adoption a *MultiMediaCard (MMC)* as the global, open standard for removable, non-volatile memory. The

⁷ <http://www.keitaide-music.org>

⁸ <http://www.mmca.org>

MMC specification defines the interface between the card (which is used for storage) and the device. *Secure MultiMediaCard (Secure-MMC)*, an MMC with cryptographic features added and secure storage for keys, is used to support digital rights management. Secure-MMC uses public key cryptography for purposes of secure transfer of content licenses, as well as for participation in other known and unknown PKI-based exchange schemes. The mobile phone, used as the playing device, is required to asymmetrically extract content licenses that are received from the license distribution center, and then symmetrically decrypt the content to be played for the consumer.

A very practical approach to Digital Rights Management is currently being developed by the OMA Wireless Applications Group, within the Download Drafting Committee. The purpose of this work is to develop an application-level protocols to provide reliable content delivery and to ensure that content will be used in a manner that is consistent with the content provider's intent. The group has entered the second phase of its work on DRM, presenting new use cases and requiring new security features. Digital signatures are expected to provide integrity protection of rights objects and their association to corresponding media content. PKI is considered the preferred option for device identification mechanism, by way of device and user certificates. OMA DRM requires the device to support application authorization mechanism, so as to prevent unauthorized entities from accessing plaintext DRM content and access rights objects. This feature can be supported through the use of application authentication through digital signatures⁹.

⁹ According to the group's concept, DRM applications require the key management to reside on the terminal.

DISCRETIX CRYPTOCELL™ AS MOBILE PKI MODULE

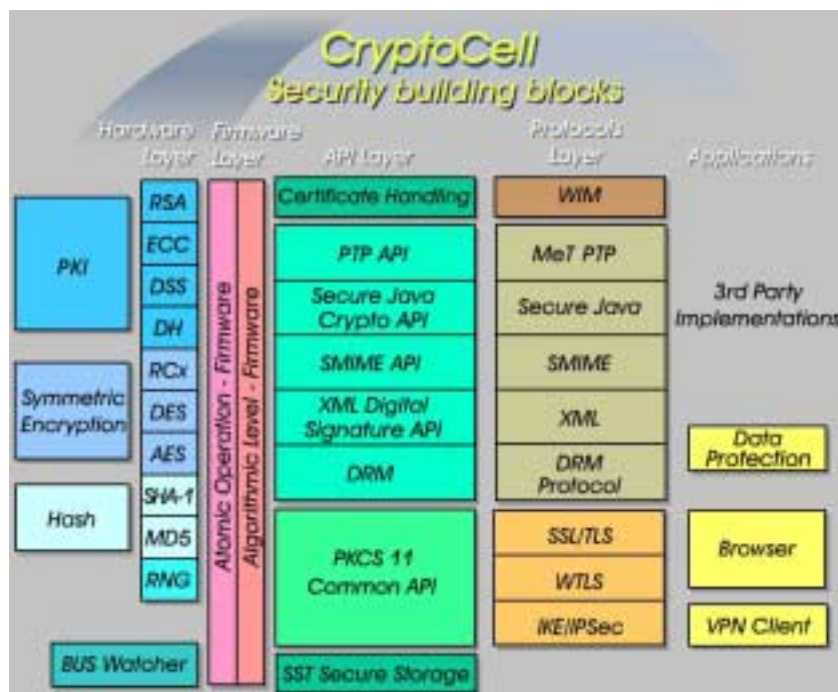
Discretix's CryptoCell technology offers a scalable, flexible and highly secured solution for mobile devices.

Discretix CryptoCell™ is an advanced embedded security engine, which resides within the base-band chip or the application processor of the mobile phone (application processors are seen in high-end phones, allowing for the support of rich-multimedia applications).

CryptoCell™ design is divided into layers, where each layer contributes to the overall uniqueness of the solution:

- Hardware modules that accelerate asymmetric and symmetric encryption algorithms.
- Cryptographic firmware library that provides access to the asymmetric (RSA, DH, DSA and ECC), symmetric (AES and DES) as well as hash (SHA-1/2, MD-5) algorithms. Implementation is always standard compliant (PKCS, NIST, ANSI etc). The firmware layer can be used by upper-layer applications by means of standard cryptographic APIs (e.g. PKCS#11) or proprietary APIs.
- A software API package that adds support for a wide range of applications, such as PTP, S/MIME, XML Digital Signature, EMV and 3Dsecure.
- A set of software modules for handling all complementary aspects of PKI, such as certificates handling, PIN handling and secure key storage.
- Software implementation of the most commonly used security protocols (SSL, TLS, WTLS and IPsec), making use of the hardware-accelerated encryption algorithms.
- High-level PKI-based applications such as Secure Actionable Alerts and Crypto-Token (a challenge-response token application).

The following diagram depicts Discretix CryptoCell layered architecture and describes the various building blocks.



ALTERNATIVE SECURITY IMPLEMENTATIONS FOR MOBILE-DEVICES

Other options for implementing security modules in mobile devices are available:

1. A removable smart card (also known as a SWIM card) that includes a functionality specified by OMA as Wireless Identity Modules (WIM). The WIM module allows for the support of specific predefined applications through a set of API functions. The major shortcoming of the SWIM card is its slow bandwidth (due to the use of legacy ISO 7816 serial interface), which inhibits the support of a wide range of applications such as VPN or secure multimedia download. Discretix CryptoCell™ provides an Embedded WIM – a WIM compliant interface to CryptoCell™ functionality, unbound to the abovementioned limitations.
2. Software-based packages, available from a variety of vendors and making use of the already limited processing power and system resources of the mobile device. These implementations cause a significant degradation to the overall user experience and are more exposed to security attacks.

About Discretix

Discretix is a semiconductor intellectual property company that develops and licenses advanced embedded security solutions for resource-constrained environments, such as wireless devices and smart-cards, where stringent limits apply to the cost, size and power consumption of the target devices.

Discretix technology has already been adopted by some of the major vendors of wireless baseband and application chipset, as well as smart-card IC vendors.



Discretix Technologies Ltd.

**Corporate
Headquarters**

43 Hamelacha Street
Beit Etgarim
Poleg Industrial Zone
Netanya 42504
Israel
Tel: +972 9 885 8810
Fax: +972 9 885 8820
Email:
marketing@discretix.com

**Representative in
Japan:**

Triangle Technologies KK
Sogo-Hirakawacho Bldg.
4F 1-4-12
Hirakawacho Chiyoda-ku
Tokyo, Japan
Tel: +81 3 5215 8760
Fax: +81 3 5215 8765
Email:
japan.info@discretix.com