Mobile Public Key Infrastructures

Ioannis P. Chochliouros
Hellenic Telecommunications Organization S.A., Greece

George K. Lalopoulos
Hellenic Telecommunications Organization S.A., Greece

Stergios P. Chochliouros
Independent Consultant, Greece

Anastasia S. Spiliopoulou
Hellenic Telecommunications Organization S.A., Greece

INTRODUCTION

During the last decade we have witnessed the widespread penetration of mobile communications infrastructures and services (Chochliouros & Spiliopoulou-Chochliourou, 2005a) together with a great expansion of various information terminals such as cell phones, notebook computers, and personal digital assistants (PDAs). Broadband facilities (Chochliouros & Spiliopoulou-Chochliourou, 2005b) have also forwarded evolutionary processes and promoted the role of the mobile sector. In particular, improved performance of cell phones and their enhanced Web-based features have resulted in their use as personal trusted devices (PTDs), in order to perform tasks such as mobile banking, stock brokering, mobile ticketing, mobile shopping, access of corporate databases, and handling of e-government procedures (e.g., completing various types of documents) (May, 2001). These must be completed in a secure and safe environment that will guarantee protection from malicious or illegal actions like spoofing—namely, stealing information concerning financial transactions (such as passwords, bank account numbers, and credit card accounts), tampering with significant documents, and so forth.

From today's perspective, network and information security (European Commission, 2001) is about ensuring the availability of services and data; preventing the disruption and unauthorized interception of communications; confirming that data sent, received, or stored is complete and unchanged; securing data confidentiality; protecting information systems against unauthorized access; and protecting against attacks (involving malicious software and securing dependable authentication—that is, the confirming of an asserted identity of entities or users). Specific security measures therefore should be taken in order to establish an appropriate environment.

BACKGROUND

PKI Technology as the Means to Ensure Security

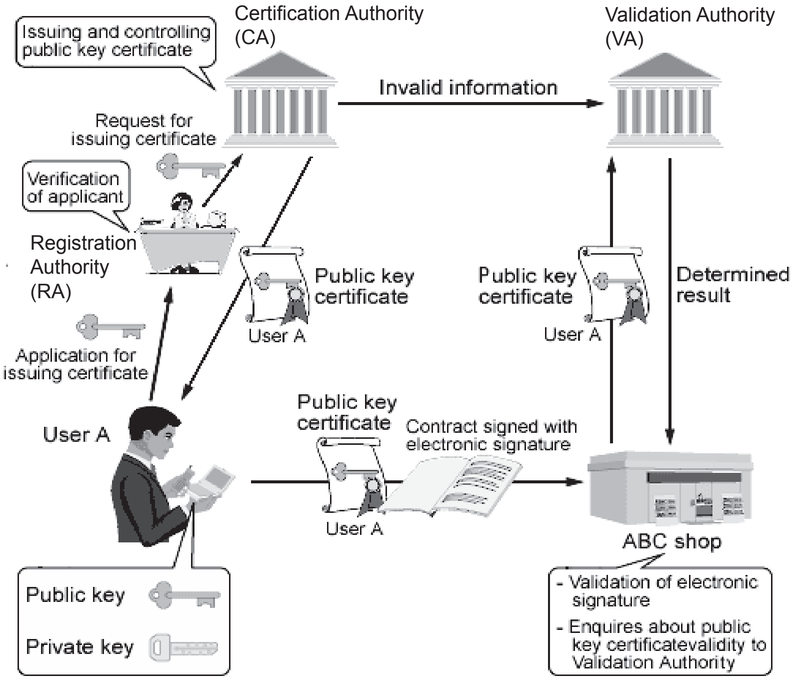
"Secure mobile transactions" implicates that, at least, the following specific features must be ensured satisfactorily:

1. **Confidentiality:** The "assurance" that information is accessible only to those parties/entities that are appropriately authorized to access it.
2. **Integrity:** The assurance that information (either stored or transmitted) has not been altered (with or without intention) between two communication points or at a given time gap.
3. **Authentication:** The assurance that the source of information is "who" it claims to be.
4. **Non-Repudiation:** The assurance that communication parties remain honest about their actions—that is, that they cannot falsely deny having originated or received information.

Public key infrastructure (PKI) is able to offer (IETF, 2005) all the above security services for the case of mobile transactions. In the following sections, we provide a more detailed explanation of PKI.

PKI is based on a main tool for encrypting and decrypting data (Adams & Lloyd, 2003), which is called a "key." In fact, public key cryptosystems use two kinds of keys: a "public key" and a "private key." The latter is held by one (legal or physical) person and is for that person's unique use only; in contrast, the former is open to the public for widespread use. In the case of authentication by a public key cryptosystem, the "person"/"entity" subject to authentication starts by encrypting the transmitted data with his private key; resulting data

Figure 1. A fundamental PKI infrastructure


Issuing and controlling public key certificate
Certification Authority (CA)
Validation Authority (VA)
Invalid information
Request for issuing certificate
Verification of applicant
Registration Authority (RA)
Public key certificate
User A
Public key certificate
User A
Determined result
Application for issuing certificate
User A
Public key certificate
Contract signed with electronic signature
User A
ABC shop
Public key
Private key
- Validation of electronic signature
- Enquires about public key certificatevalidity to Validation Authority

cannot be read, unless a great deal of complex decryption is done; in fact, it cannot even be read by the person who encrypted it. Next, the "entity" realizing authentication uses the public key for data to decryption, and so information returns to a "readable" status. If data is correctly decrypted, the performer concludes that the key used for the encryption purposes was the private key that corresponds to the public key; consequently, the "person" who encrypted the data must be the holder of the private key. A fundamental question that raises here regards the case in which the entity performing the authentication mistakes the holder of the private key. Whether the encrypted transmitted data can be decrypted correctly simply depends on the specific nature of the public key corresponding with the private key. On the other hand, if the public key belongs to a complete "stranger" but does correspond to the proper private key, the stranger can decrypt the encrypted transmitted data. Therefore, authentication of a legitimate person can be mistaken, and it is possible that someone can pretend to be someone else.

The above-described scenario means that in the case of authentication through a public key cryptosystem, it is extremely important to correctly connect the right person and the public key. Consequently, it has become essential to devise a system that can certify, by means of utilizing a third-party organization with no direct connection to the person undergoing authentication, whether the person in question is unmistakably the person holding the corresponding private key or whether that person is a malicious "stranger" intending to spoof the cryptosystem. This scheme is called PKI, which practically constitutes a core technology that configures the security infrastructure for protecting electronic commerce (e-commerce), especially in the mobile sector (Lalopoulos, Chochliouros, & Spiliopoulou-Chochliourou, 2005).

A Social System for Supporting PKI Implementation

A commonly accepted configuration of a proper social system for the efficient support of PKI perspective is described (Kaji, 2004) in Figure 1.

Figure 1 shows the separate roles of various organizations, authorities, and other entities involved in authentication and certification procedures within a PKI system.

The first key-concept, a so-called certification authority (CA), confirms "who" is the owner of the private key corresponding to the public key and fixes the "prescribed" correspondence between them. According to existing regulatory provisions and practices (European Parliament and Council of the European Union, 2000), CAs can be public or private organizations. The CA then issues (and controls) an "electronic certificate" as the authorization of this correspondence. A registration authority (RA) is an organization responsible for verifying the identity of the key holder and checking his certification with the CA.

The second key-concept is the validation authority (VA), a body for checking the legality of electronic certifi-