Mobile Payment

Gyõzõ Gódor
Budapest University of Technology and Economics, Hungary

Zoltán Faigl
Budapest University of Technology and Economics, Hungary

Máté Szalay
Budapest University of Technology and Economics, Hungary

Sándor Imre Dr.
Budapest University of Technology and Economics, Hungary

INTRODUCTION

The widespread usage of new telecommunication technologies implies the demand on payment via Internet since the '90s. First, these solutions were applied only by pioneer users, while average men still chose traditional payment methods such as payment by cash, cheque, or bank transfer. In the latest decade, the notable improvement of mobile communications allowed the provision of customized services. A new payment method has appeared which is called mobile-payment. Consequently, increasing number of banks provide access to their services via mobile equipment.

Reliable network security is an essential prerequisite for the expansion of the rapidly growing world of electronic payment. Public key infrastructure (PKI) offers the capabilities needed to provide this security. Establishing trust in a wireless public key infrastructure (WPKI) is crucial for the success of applications that will exploit the opportunities created by handheld wireless devices. This trust is based on the reliability of the technology but also on a carefully implemented system of laws, policies, standards, and procedures.

The development of trusted electronic transactions is motivated by legislation. The EU adopted a legislative framework to guarantee the security and acceptance of electronic signatures in 1999. The U.S. adopted legislation for the recognition of electronic signatures in national and global trade in June 2000 (Sievers, 2000).

This article deals with mobile payment and mobile banking services and focuses particularly on the mobile side of the system. First, we introduce the technological background necessary for developing m-services, and we define the m-payment reference model. After that, the differences between chip-card and software based implementations will be presented. Finally, we conclude the article and summarize the main terms used in the article.

BACKGROUND

The Mobile Payment Forum (MPF) (2002) defines mobile-payment (m-payment) as the process of two parties exchanging financial value using a mobile device in return for goods or services. The trusted transactions of a mobile payment system are called mobile payment transactions. The main areas of use are the following:

- m-banking and m-payment, in case of performing banking and payment affairs;
- m-administration, when accomplishing administration tasks; and
- m-government, in case of arranging public administration affairs using the mobile electronic way.

The mobile device and the mobile network have two main roles in m-payment:

- they enable secure client authentication and identification; and
- they support the generation of digital signatures on the client side.

The user authentication means that a service provider determines the identity of a user (Kanniainen, 2001).

The digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures can be used for many purposes, such as authorizing a subsequent transaction or creating a signature of the user with properties fulfilling the requirements of electronic signature laws.

The user authorization means that a service provider ensures that the user has viewed and accepted a transaction contract (Kanniainen, 2001).

The technological background exists for developing services based on trusted mobile transactions. The bandwidth of the mobile channel is only a small fraction of that of the Internet, but user authentication, digital signature transfer, authorization control require low bandwidth from the mobile network. Even low-end mobile devices support WAP functionalities (Wireless Application Protocol Forum [WAP Forum], 2001c) and text message sending. Their SIM card implements SIM Application Toolkit (SAT) and supports the necessary cryptographic algorithms at chip-card level. These are essentials to implement client-side banking applications (Van der Merwe, 2003).

Smart-phones with increased processing speed have already been introduced to the market. They support the development of software-based banking applications without using the functionalities of chip-card and relying only on the security of software-based encryption algorithms (Mobey Forum Mobile Financial Services Ltd. [Mobey], 2003).

In 2004 the Trusted Mobile Platform was introduced by IBM and Intel. It is a software and hardware requirement specification for mobile equipment (Trusted Mobile Platform, 2004) in secure environment.

Trusted mobile services are based on PKI technology. PKI offers strong authentication and encryption mechanisms and facilitates the secure exchange of sensitive messages in public information networks (Torvinen, 2000). PKI functions permit detection of messages that have been tampered with or altered during transmission. PKI summarizes the processes and techniques performing key-certification in public cryptography architecture. Each entity in the PKI system has at least one key-pair which consists of a private key and a public key. The private key is the secret of a given entity never discovered to others. Public keys are certified by a trusted third party called Certification Authority (CA) (WAP Forum, 2001a).

WPKI is a PKI where at least the user-side of the system uses wireless medium. WPKI uses more compact certificates then PKI and its certificate acquisition process is adapted to mobile environment (WAP Forum, 2001b).

Several international technical organizations were founded starting from the late ’90s, elaborating standard solutions or directives for trusted mobile transactions. Such organizations are Radicchio, Liberty Alliance, GSMA, ETSI M-COMM Working Group, OMA, MPSA, Mobey Forum, and Mobile Payment Forum, for example. Members of these organizations are mobile operators, financial institutions, research, developing, and standardization organizations (see Table 1).

Table 1. Organizations specifying trusted mobile transactions

Name	Foundation	Members
Radicchio (T2R)	Mars 2002	GSMA, Liberty Alliance, ETSI
Liberty Alliance	Sept 2001	VeriSign, Nokia, Sun, RSA, Vodafone, American Express, Novell
MPSA (SimPay)	Mars 2003	Vodafone, T-Mobile, Orange, Telefónica Móviles
Mobey Forum	Mai 2000	VISA, ABN-Amro Bank, Nokia, Deutsche Bank
MeT	April 2000	NEC, Nokia, Panasonic, SonyEricsso2n
Mobile Payment Forum (MPF)	Nov. 2001	American Express, JBC Co. Ltd., MasterCard International and Visa International
Open Mobile Alliance (OMA)	June 2002	Vodafone, Ericsson, WAP Forum, IT companies

MOBILE-PAYMENT SERVICES

An m-payment system involves a wireless device that is used and trusted by the customer. M-payment is not a new payment instrument but an access method to activate existing payment transactions processed by banks.

Mobile payment transactions (and systems) can be classified upon location basis or value basis. On location basis, local and remote environments are distinguish (Mobile electronic Transactions [MeT], 2001), on value basis, micro (<10Euros) and macro (>10Euros) payment (Mobey, 2003). In local environments transactions are usually initiated over a short-range wireless technology such as Bluetooth or RFID (Saleem, 2002). A typical application would be retail shopping using an account-based payment made from a mobile device. In remote environment the connection between the content server and mobile device is established via a Public Land Mobile Network, such as the GSM cellular network (Mobey, 2003).

The four main parties involved in a mobile payment transaction (see Figure 1)—the user, the network operator, the financial institution, and the merchant—share many of the same concerns that need to be addressed by a mobile payment standards body (Henkel, 2001; MPF, 2002).

- Consumers are mostly concerned with security, ease of use, and privacy. They also require the payment scheme to work across multiple devices, including mobile phones, PDAs, wireless tablets, and handheld computers.
- Mobile operators’ principal concerns revolve around standardization and interoperability. Operators want payment to be seamless, allowing them to compete on services and applications.