# Study of mobile payment protocols and its performance evaluation on mobile devices

Rafael Martínez-Peláez* and
Francisco J. Rico-Novella

Technical University of Catalonia,
Department of Telematic Engineering,
Jordi Girona Road, Campus Nord, Block C3,
Barcelona 08034, Spain
E-mail: rafaelm@entel.upc.edu
E-mail: f.rico@entel.upc.edu
*Corresponding author

Cristina Satizábal

Pamplona University,
Engineering and Architecture Department,
Km 1 via Bucaramanga – Pamplona,
Pamplona, Colombia
E-mail: isabel.satizabal@unipamplona.edu.co

**Abstract:** Mobile payment protocols must provide security services (e.g., authentication, authorisation, integrity, privacy and non-repudiation), but the features of mobile devices make it a difficult task, especially when the service requires to perform public key operations. It is very well known, that the public key operations require high execution time of the CPU and battery consumption. In this paper, we computed the computational cost required by each entity in five mobile payment protocols. In addition, we computed the transmission time of each message among different entities. The exchange of message was done using Bluetooth technology. The performance evaluation of each mobile payment protocol defines its feasibility according with the whole time expending during the protocol considering its computational cost and transmission time.

**Keywords:** computational cost; Bluetooth; transmission time; m-payment protocols.

**Reference** to this paper should be made as follows: Martínez-Peláez, R., Rico-Novella, F.J. and Satizábal, C. (2010) 'Study of mobile payment protocols and its performance evaluation on mobile devices', *Int. J. Information Technology and Management*, Vol. 9, No. 3, pp.337–356.

**Biographical notes:** Rafael Martínez-Peláez received his degree in Computational System Engineering from the University of the Valley of Mexico (México) in 2004. Currently, he is carrying out a PhD in Telematics Engineering at the Technical University of Catalonia (Spain). His main areas of interest are electronic and mobile payment systems, and applications of smart card and biometrics with security protocols design.

Francisco J. Rico-Novella received his degree in Telecommunication Engineering and his PhD from the Technical University of Catalonia in 1989 and 1995, respectively. Presently, he works in the Department of Telematic Engineering with the Telematics Services group. His current research interests include network security and electronic commerce.

Cristina Satizábal received her degree in Electronic and Telecommunications Engineering from Cauca University (Colombia) in 2000 and her PhD in Telematics Engineering from the Technical University of Catalonia (Spain) in 2007. Currently, she is a part of the Engineering and Architecture Department of Pamplona University (Colombia) and belongs to LOGOS research group. Her research interest includes public key infrastructure (PKI), privilege management infrastructure (PMI) and intrusion detection systems (IDS).

## 1 Introduction

In the last few years, the boom of mobile payment has had four main protagonists: the constant growth of mobile communication systems, more and more mobile devices with better characteristics such as storage capacity, processing power and communication capabilities, new business environment focused in mobile users and Java platform for mobile devices.

Since the process of payment can be achieved between the customer and a point of sale (merchant) or between unknown entities and the payment information is sent through an open communication (e.g., Bluetooth, infrared), entities can be victims of fraud. For those reasons, mobile payment protocols must offer a high level of security. Traditionally, cryptographic operations are used to provide security services such as authentication, integrity, privacy and non-repudiation. However, some cryptographic algorithms require high computationally processing and battery.

Previous works have examined mobile payment protocols. Research has been focused on studying the state of the art (Choi et al., 2006; Wrona et al., 2001). Heijden (2002) examined the successful factors of mobile payment systems. Also, Das et al. (2005) have composed a security framework for ad hoc mobile payment. The performance of cryptographic operations on mobile devices have examined by Argyroudis et al. (2004), Martínez-Peláez et al. (2008), Satizábal et al. (2007a, 2007b) and Tillich and Grobschädl (2004).

In this paper, we carry out an evaluation of different mobile payment protocols to determine its performance based on two key points: computational cost and transmission time, in order to know if new mobile devices can perform the next generation of payments. We have considered the whole execution time of each protocol to determine its feasibility.

The remaining part of the paper is structured as follows. Section 2 presents a literature review of mobile payment. Bluetooth technology is described in Section 3. In Section 4, we provide a detailed description of the WPKI. We provide a brief overview of the five mobile payment protocols that we have evaluated in our study in Section 5. In Section 6, we present the methodology used in our study. The results of our performance evaluation are presented in Section 7. Section 8 concludes.

## 2 Mobile payment: a literature review

Mobile payment is defined as the process of exchanging financial values between two parties using a mobile device to pay for products or services (Nambiar et al., 2004). With this new payment option, customers can pay for products and services anywhere and anytime with the comfort offered by their mobile devices.

### *2.1 Mobile payment scenarios*

Customers can participate in three types of mobile payment scenarios to purchase products or services (Delic and Vukasinovic, 2006; Gao et al., 2005).

- Real point of sale (POS): each customer interacts with a vendor machine (merchant) using his/her mobile device. The communication between the vendor machine and customer is using wireless technology such as Bluetooth or infrared. There are two subdivisions:
  - Complete customer-to-vendor machine mobile commerce transaction, which enable customers to purchase and pay for products or service without the participation of other person.
  - Partial customer-to-vendor machine mobile commerce transaction, which enable customers to complete the purchase process with the assistance of other person and the payment process with the vendor machine.
- Virtual POS: this scenario is designed to take advantage of web connections through 3G communication systems by enabling mobile commerce into mobile devices. In this scenario, wireless application protocol (WAP) is frequently used to establish a transmission between the mobile device and web server. Web servers allow customers to receive web content in their phones such as rings, music and video.
- Peer-to-peer (P2P): customers and merchants interact using their mobile devices to complete a commerce transaction. In this scenario, customers and merchants take advantage of different wireless technologies and applications to complete the transfer of funds. The main difference with other scenarios is the absences of static role for each user, in one case a user can participate as customer while in the next time participate as merchant.

### *2.2 Payment medium*

Mobile payment protocols inherited types of payment from electronic payment protocols such as credit card schemes. Mobile payment protocols can be classified according to the basis of payment (Delic and Vukasinovic, 2006; Gao et al., 2005) as follows.

#### *Bank account*

Customers must have a credit or debit card associated with a specific bank account. Customer discloses the information printed on the card such as card number, CVV2, expiration date and name of merchant. Then, the merchant forward the information to

trusted third party (TTP). Finally, the TTP transfers the total amount of payment from customer's bank account to merchant's bank account.

### *Electronic cash*

Customer must establish a business agreement with a TTP, called payment gateway. The main function of the payment gateway is to convert real money to their electronic equivalent. Then, the electronic cash must be stored in a secure device like smart card or SIM to avoid frauds. The electronic cash have monetary value supported by financial institutions.

### *Phone bill*

Customer should have a business agreement with a cell phone service provider. The business agreement consists of two parts:

1 cell phone service provider gives credit to customer for making calls and paying for goods or services

2 customer pays the bill every month.

## *2.3 Time of payment*

We define time of payment as the moment when the customer transfers funds from his account to other account (Panurach, 1996; Wrona et al., 2001).

- *Pre-paid:* customers transfer funds in advance to have credit in order to obtain products or services.
- *Post-paid:* customers obtain products or services before transferring funds.
- *Real-time:* customers transfer funds immediately when they purchase a product or service.

## *2.4 Security*

Mobile payment protocols must offer robust security because the financial data are sending over wireless networks. In this sense, customers and merchants require mutual authentication, payment authorisation, confidentiality, integrity and non-repudiation (Heijden, 2002; Shon and Swatman, 1998). We describe the security factors as follows:

- *Authentication:* mobile payment systems must offer the option to authenticate each entity (mutual authentication).
- *Authorisation:* mobile payment systems should request confirmation of the payment.
- *Integrity:* mobile payment systems must guarantee that the messages have not been modified.
- *Non-repudiation:* mobile payment systems should avoid refuting payments.
- *Privacy:* mobile payment systems must avoid eavesdroppers have access to the messages.

### *2.5 Mobile payment technology*

Software development and wireless technologies are used to develop mobile payment systems.

Java 2 Micro Edition (J2ME) is a group of specifications that can be used to develop Java applications for mobile devices. The J2ME applications can run on mobile devices with low processing power and storage capacity because the platform is independent of the device. J2ME requires the use of a virtual machine called kilobyte virtual machine (KVM). The KVM maintains all the central aspects of the Java programming language in a small range of memory (around 40 KB to 80 KB).

Short message service (SMS) is a service to send text messages among mobile phones and over different mobile communication systems (GSM, UMTS). The maximum length of a message is around 150 characters. The messages are not transferred in real time.

WAP is an open standard developed to programme information services and telephony for digital mobile phones and other mobile devices. The mobile devices can read the internet content in a special format. WAP uses binary transmission for a greater data compression. It is optimised for high latencies and low bandwidth. In addition, it includes authentication and encryption/decryption options.

Infrared is a wireless technology to interconnect mobile devices with each other or with other devices via point-to-point communications. Infrared technology transfers voice and data in real time. The transmission area needs line of sight and its transfer rate is 4 Mbps.

## 3 Bluetooth technology

Bluetooth is a wireless technology to interconnect mobile devices with each other or with other devices via point-to-many or point-to-point communications. This technology transfers voice, data and video in real time. The transmission area is omni-directional and its transfer rate is 1 Mbps. The maximum distance between the data origin (source) and receiver is around 10m. Bluetooth technology transmits and receives on frequency band 2.45 GHz. Bluetooth technology is a key element in the mobile commerce because it enables mobile devices to pay for products or services (Bruno et al., 2002; Ferro and Potorti, 2005).

### *3.1 Baseband layer*

Bluetooth technology uses two types of link to establish a connection among devices: synchronous connection oriented (SCO) and asynchronous connectionless link (ACL). SCO link establishes a point-to-point connection and is a symmetric dedicated link between two devices. On the other hand, ACL link establishes a point-to-multipoint connection and is an asynchronous link among all the devices. The first type of link is a circuit switched connection between the master and slave, while ACL link is a packet switched connection among the master and all the slaves. SCO link guarantees the delay and bandwidth to transmit an average quality of voice and music by the use of the link management protocol (LMP). LMP performs the link configuration such as quality of service (QoS) (Ferro and Potorti, 2005).

ACL links are appropriate for non-real time transmission data. This means that, applications with different QoS parameters cannot be supplied. There are two different ACL link packets (frames):

1 DMX, where the payload is encoded

2 DHX, where the payload is unprotected.

The value of 'X' stands for the number of slots required to transmit the frame. DMX types are DM1, DM3 and DM5, which includes forward error correction (FEC), cyclic redundancy check (CRC) code and automatic repeat request (ARQ). The payload header is one or two bytes long, depending on the packet type and its specification, such as logical channel, user payload length and flow control. Table 1 summarises the DMX and DHX link packets (Bruno et al., 2002).

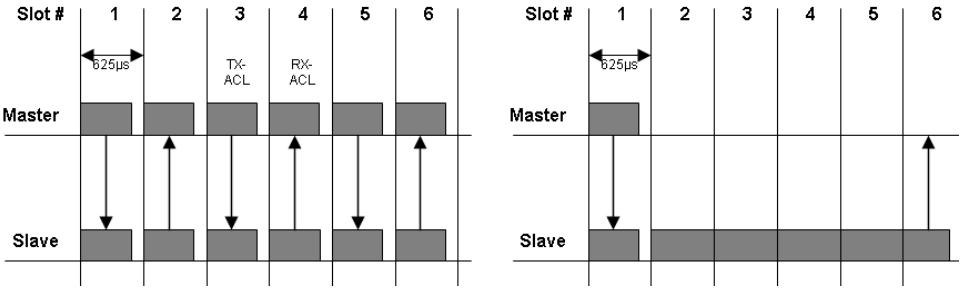
**Table 1** Characteristics of ACL packets

| *Type* | *User payload (bytes)* | *FEC* | *CRC* | *Symmetric max rate (Kbps)* | *Asymmetric max rate (Kbps)* | |
|---|---|---|---|---|---|---|
| | | | | | *Forward* | *Reverse* |
| DM1 | 0–17 | 2/3 | Yes | 108.8 | 108.8 | 108.8 |
| DM3 | 0–121 | 2/3 | Yes | 258.1 | 387.2 | 54.4 |
| DM5 | 0–224 | 2/3 | Yes | 286.7 | 477.8 | 36.3 |
| DH1 | 0–27 | No | Yes | 172.8 | 172.8 | 172.8 |
| DH3 | 0–183 | No | Yes | 390.4 | 585.6 | 86.4 |
| DH5 | 0–339 | No | Yes | 433.9 | 723.2 | 185.6 |

## *3.2 Physical layer*

Bluetooth technology transmits and receives on the frequency band of 2.4 GHz. The band is divided into 79 MHz wide channels that are spaced by 1 MHz. This layer utilises frequency hopping spread spectrum (FHSS) as technique of transmission. FHSS can reduce the impact of jamming and interference caused by other systems. The transmission channel changes 1,600 times per second.

**Figure 1** An example of packet transmission: single-slot and multi-slot packet



Bluetooth technology uses a slotted time division duplex (TDD) scheme for duplex transmission, where each time slot is 625 μs. Each slot corresponds to a different transmission. The master uses the even numbered time slots to transmit, while the slaves use the odd numbered time slots (Ferro and Potorti, 2005). Figure 1 illustrates the packet transmission in an ACL link (single-slot and multi-slot packet).

## 4 WAP public key technology (WPKI)

WPKI is an optimised extension of the typical PKI for the wireless environment. It has optimised the protocols (WML and WMLScript) and the format of the certificates (WTLS certificates). The goal of WPKI is to reuse existing PKI standards where available and only develop new standards where necessary to support the specific requirements of WAP. The general model adopted in the current version of WPKI is, according to WAPForum (2001a):

- WTLS server and root certification authority (CA) certificates stored in the device will be according to WTLS certificate defined in WAPForum (2001b).
- Client (WTLS and application) and root CA certificates stored in servers will be according to X.509 as profiled in Houseley et al. (1999).
- Client (WTLS and application) and root CA certificates which must be sent over the air and/or stored in WAP client devices will be according to X.509 as profiled in WAPforum (2001).
- Storage of the certificate URL in the device, rather than the full client certificate, is the preferred model when X.509 format certificates would otherwise be expected to be transferred over the air. Storage of X.509 client certificates in the device is expected to be the exception, unless they are provisioned on the device, through a wireless identity module (WIM).

WPKI requires the same components used in typical PKI: CAs, registration authorities (RAs), end entities (EEs), PKI directories (DIRs) and add a new component, called PKI portal. The PKI portal is responsible for translating requests made by the WAP client to the RA and CA in the PKI. The PKI portal will typically embed the RA functions and interoperate with the WAP devices on the wireless network and the CAs on the wired network.

### *4.1 Certification path validation*

A certification path is a chain of public key certificates through which a user can obtain the public key of another one. The primary goal of the path validation is to verify the binding between the client and his/her public key. A trust anchor is the CA verification key used by the client application as the starting point for all certificate validation. The certification path length is equal to the number of certificates in the path that is the number of CAs in the path plus one. Since the verifier knows and trusts the public key of his/her trust anchor, the trust anchor's certificate is not included in the path (Satizábal et al., 2007a). In general, the path validation process involves the following steps:

- *Discovering a certification path:* it is to set up a trusted path between the verifier's trust anchor and the target entity based on the trust relationship among the entities of the PKI.
- *Retrieving the certificates:* it is to retrieve each certificate in the path from the directories where they are stored.
- *Verifying the digital signatures:* it is to verify the validity of the digital signature of each certificate in the path. It involves:
  - decrypting the signed part of the certificate with its issuer's public key
  - computing the hash of the certificate's content
  - if the result of steps *a* and *b* are the same then the signature is valid.
- *Verifying the validity of the certificates:* it is to determine if the certificates are expired or revoked. The certificates validity period is used to verify the expiration, while the revocation status depends on the revocation mechanism.

### *4.2 Hierarchical architecture*

In a hierarchical architecture, all the users trust the same root CA (RCA). That is, all the users of a hierarchical PKI begin certification paths with the RCA public key (Satizábal et al., 2007a). In general, the RCA does not issue certificates to users but only issues certificates to subordinate CAs. Each subordinate CA may issue certificates to users or another level of subordinate CAs, if it is permitted by policies.

The certification paths are easy to build in a hierarchical PKI because they are unidirectional and the longest path is equal to the depth of the tree plus one: a CA certificate for each subordinate CA plus the user's certificate.

## 5 Cases of study: five mobile payment protocols

Our study includes the analysis of five mobile payment protocols, developed in the last years. Table 2 shows the mobile payment scenario (MPS), payment medium (PM), type of payment (TP) and security. For more information about the protocols, see references.

**Table 2** Five mobile payment protocols developed for mobile devices

| *Protocol* | *MPS* | *PM* | *TP* | *Security* |
|---|---|---|---|---|
| Virtual POS | Virtual POS | Bank account | Post-paid | Authentication |
| | | | | Integrity |
| | | | | Non-repudiation |
| | | | | Privacy |
| Real POS | Real POS | Bank account | Post-paid | Authentication |
| | | | | Integrity |
| | | | | Non-repudiation |
| | | | | Privacy |

**Table 2** Five mobile payment protocols developed for mobile devices (continued)

| *Protocol* | *MPS* | *PM* | *TP* | *Security* |
|---|---|---|---|---|
| Anonymous payment | Real POS | Bank account | Post-paid | Authentication |
| | | | | Integrity |
| | | | | Non-repudiation |
| | | | | Privacy |
| KSL | P2P | Bank account | Post-paid | Authentication |
| | | | | Integrity |
| | | | | Non-repudiation |
| | | | | Privacy |
| M-cash model | P2P | Electronic cash | Real time | Authentication |
| | | | | Integrity |
| | | | | Non-repudiation |
| | | | | Privacy |

## *5.1 Virtual POS protocol*

Virtual POS protocol has been developed for providing user authentication, integrity, non-repudiation and privacy (Hassinen et al., 2006). In order to provide user authentication, the scheme uses PKI SIM cards. The PKI structure is provided by the Finnish Population Register Centre. The centre issues certificates for authentication and encryption and non-repudiation. The private keys are stored in the SIM card. The user is authenticated before his/her SIM card by a PIN code. Each user of the system has a unique Finnish Electronic User ID. This protocol is based in the use of a credit card as payment medium and it was develop to operate over IP-based data transfer (e.g., GPRS).

This protocol takes advantage of the PKI services, for that reason, customer and merchant perform several cryptographic operations such as encryption/decryption and digital signature creation/verification.

The authentication process is not defined here. We suppose that the authentication process uses certification path validation described in Section 4.

## *5.2 Real POS protocol*

This protocol has been developed for real POS scenario (Hassinen et al., 2006). The medium of payment is a credit card. The mobile device must support J2ME as the programming platform. This protocol takes advantage of PKI services to provide user authentication, integrity, privacy and non-repudiation. The scheme uses PKI SIM cards to store the keys and the certificates issued by Finnish Population Register Centre. The centre issues certificates for authentication and encryption and non-repudiation. The private keys are stored in the SIM card. The user is authenticated in front of his/her SIM card by a PIN code.

In order to carry out the authentication process, the customer uses the online certificate status protocol (OCSP). Because the terminal does not have a connection to the internet, it cannot provide the authentication of the customer's certificate, the customer

must provide proofs about the validity of his/her certificate. The customer and terminal perform several cryptographic operations.

### 5.3 Anonymous payment in a kiosk centric model

This protocol has been developed with the aim to provide a mobile payment system where the customer cannot communicate with the issuer due to the absence of internet access (Isaac et al., 2006). In addition, the protocol maintains the anonymity of the customer using nicknames instead of client's real identity. This protocol uses a credit or debit card as PM and Bluetooth as wireless technology.

In the first phase, the customer creates several nicknames that are known only by the customer and issuer, and shares his/her credit or debit card information with the issuer. According to the operation model, the scheme requires the use of self-certified to provide an authentication encryption scheme without the use of traditional certificate and PKI infrastructure.

In the second phase (payment phase), the customer and merchant are not authenticated. The customer must send the payment information through the merchant with the following features:

- resistant to attacks while in transit
- recoverable only by the issuer
- able to assure that it has been created and sent by the customer.

The protocol achieves the following security features: anonymity (the customer does not disclose his/her identity to the merchant), confidentiality (the data are encrypted), integrity (the data are singed) and non-repudiation (the digital signature establishes a relationship between the signer and the owner of the key).

### 5.4 KSL protocol

This protocol has been developed with the aim to reduce the number of public key operations, carried out by the customer (Kungpisdan et al., 2003) in other proposals such as SET protocol. This protocol is based on the use of a credit card as PM and it can operate over different wireless technologies. Although the customer does not perform any public key operation, the protocol satisfies the following security requirements: authentication, integrity, confidentiality and non-repudiation.

The registration phase is the first step. The customer needs to register himself/herself to the issuer. This process can be achieved via website or phone. After the registration, the client receives wallet software and he/she can generate a secret key shared $Y$ between the customer and issuer. Then, the customer and merchant must establish a secret key shared $X$. After this process, the customer and merchant can initialise the payment process. At this point, it is obvious that both customer and merchant must maintain a large number of keys, this relation is given by $n–1$, where $n$ is the total number of customers with whom the merchant has a business relationship or the number of merchants which the customer has a business relationship.

In the payment phase, the exchange of messages between the customer and merchant are encrypted using the secret key $X$. In addition, the payment information is encrypted

with *Y* that was created in previous phase between the customer and issuer; this means that only the owner of *Y* can decrypt the payment information.

### *5.5 M-cash model: a script anonym*

This protocol has been developed with the aim to provide an alternative PM instead of a credit or debit card (Martínez-Peláez and Rico-Novella, 2006; Martínez-Peláez and Rico-Novella, 2006a). M-cash is the digital version of the traditional cash. Customers can purchase goods or services of low value and the merchants reduce the cost per transaction.

Because the m-cash is the digital version of paper money, it must contain security characteristics to avoid frauds such as, double spending and forgery. This means that the m-cash requires additional security features than protocols based on credit or debit cards.

In this protocol, the authentication between the customer and merchant is achieved by means of their certificates. Then, they can establish a secure channel for future communication.

This protocol requires low number of public key operations, because the information exchange between the customer and merchant is encrypted using a symmetric key. Before the customer must pay the total amount, he must compute the hash chain function to create the m-cash. Then, the merchant verifies the validity of the m-cash and forward it to the payment gateway.

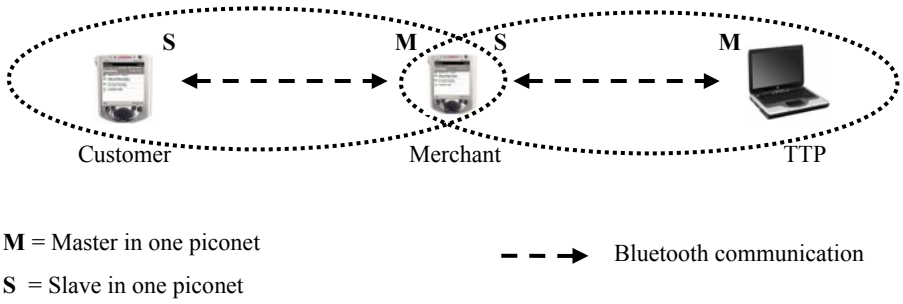
## 6 Methodology: scenario and data packet characterisation

In this section, we define the methodology used to carry out the performance evaluation of different mobile payment protocols in mobile devices.

### *6.1 Scenario*

A mobile device with Bluetooth may operate in either master or slave mode. In the scenario defined in this paper, the merchant operates in master mode while the customers operate in slave mode, which is the simplest configuration of a Bluetooth network, as shown in Figure 2. Other piconet is built between the merchant and the TTP. In this case, the TTP can be a payment gateway or bank.

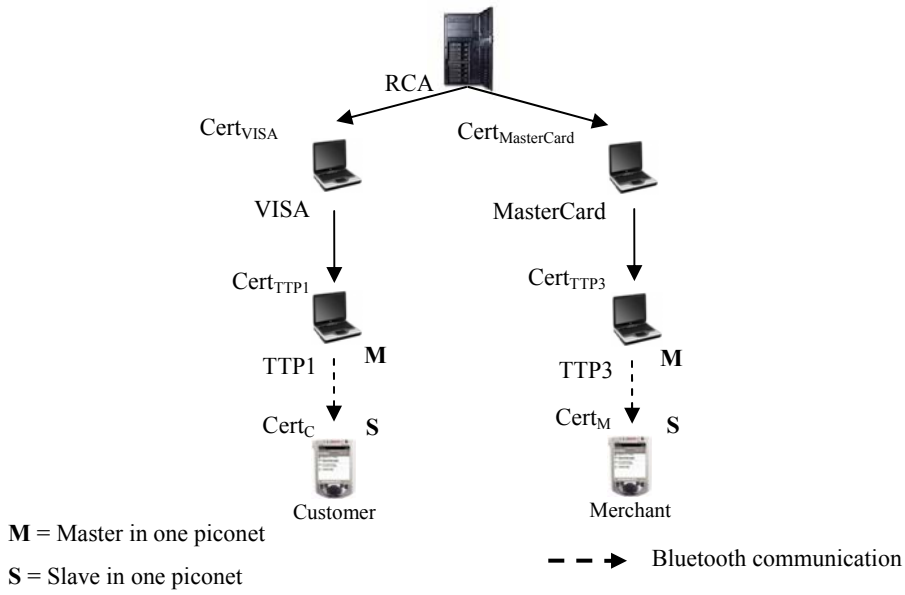
**Figure 2** P2P scenario: two piconet configurations



When the protocol requires mutual-authentication by means of digital certificates (e.g., Virtual POS, Real POS and M-cash protocols), we suppose a hierarchical PKI that involves the following entities (see Figure 3):

- *Root certification authority (RCA):* it could be a national or international certification authority, such as VeriSign.
- *Credit card certification authority (CCCA):* it could be an international credit card company such as VISA or MasterCard. CAs issue certificates to TTPs
- *Trusted third party (TTP):* it is the CA of some e-commerce application service provider. A TTP acts like mediator between the customer and merchant and issues certificates to users (customers and merchants). The TTP can be a payment gateway or bank issuer.
- *Customer (C):* is a user that wants to obtain some object or service from a merchant.
- *Merchant (M):* is a user that offers its products or services to the customers.

**Figure 3** PKI structure




## *6.2 Data packet characterisation*

A realistic characterisation of the traffic is quite difficult due to the lack of an exact knowledge of the packets' length transmitted during the operation of each message. For that reason, we set the length of each packet transmitted between the customer and merchant in a piconet scenario. We decided to use DH5 packets in the analysis.

The maximum size of the DH5 payload is 339 bytes and each ACL packet fits into five slots. When a packet arrives to the Bluetooth baseband layer, its payload consists of three parts:

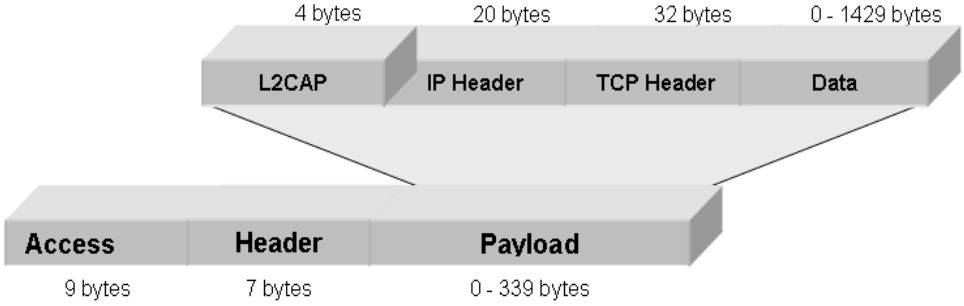
1 an IP header with 20 bytes

2 a TCP header with 32 bytes

3 a data with variable length.

In addition, L2CAP adds 4 bytes as channel identification and packet length (Bruno et al., 2002; Ferro and Potorti, 2005). The format of ACL packets is shown in Figure 4. Therefore, the maximum length of a packet is 355 bytes.

**Figure 4** ACL packet structure




## 7 Performance evaluations

### *7.1 Transmission time*

We assume an ideal channel without packet lost and we consider a multi-slot packet transmission.

In order to initialise a new communication, the master device uses the inquiry procedure (Inq_p) and page scheme (Pag_s) to discover and establish a new communication with slave devices. The average time for the inquiry phase is 0.71s and 0.64s for the page phase (Ferro and Potorti, 2005).

Let us introduce some notation adopted in this paper. For the total size of the packet $L$, we denote with $U$ the payload of each ACL packets (type DH5). We will refer to the number of ACL packets with $N_{DH5}$, so that; we have equation (1):

$$N_{DH5} = L / U \tag{1}$$

Now we can determine the delay ($D$) caused by the segmentation on TCP layer ($TCP_D$), IP layer ($IP_D$), L2CAP layer ($L2CAP_D$) and Baseband layer ($Base_D$) using equation (2), where its values are 1µs, 1µs, 1ms and 1ms, respectively (Johansson et al., 2000).

$$D = TCP_D + IP_D + L2CAP_D + Base_D \tag{2}$$

Furthermore, we indicate with $S_T$ the total number of slots used to transmit the ACL packets. We have equation (3):

$$S_T = [(N_{DH5} * DH5 / 1) + (N_{DH5} * DH5 / 5)] - 1 \quad (3)$$

After we obtained the $S_T$, we know the total number of slots used to transmit the ACL packet and the slots empty. The whole transmission time (TT) to transmit each message is given by equation (4), where $T_{SLOT}$ is the transmission frequency (625 μs).

$$T_T = (ST * T_{SLOT}) + D \quad (4)$$

Thus, equations (1) to (4) are use to obtain the transmission time of each messages exchanged among the entities in the five mobile payment protocols. We have assumed the data field size in each case. In Section 6, we described the data packet characterisation used in our performance evaluation.

Tables 3, 4, 5, 6 and 7 summarise the transmission time for each message exchanged among the entities in the Virtual POS protocol, Real POS protocol, anonymous payment protocol, KSL protocol and M-cash protocol, respectively.

**Table 3** Parameters: transmission time in Virtual POS protocol

| *Message* | | *Data (bytes)* | *Packet length L (bytes)* | *ACL packets* $N_{DH5}$ | *Slots* $S_T$ | $T_T$ *(s)* | *Whole time (s)* |
|---|---|---|---|---|---|---|---|
| 1 | Inq_p and Pag_s | – | – | – | – | 1.35 | |
| 2 | C to M | 500 | 556 | 2 | 11 | 0.0088 | |
| 3 | M to C | 6,800 | 6,856 | 21 | 125 | 0.0881 | |
| 4 | C to M | 7,920 | 7,976 | 24 | 143 | 0.0993 | 1.590 |
| 5 | M to TTP | 2,480 | 2,536 | 8 | 47 | 0.0333 | |
| 6 | TTP to M | 256 | 312 | 1 | 5 | 0.0051 | |
| 7 | M to C | 256 | 312 | 1 | 5 | 0.0051 | |

**Table 4** Parameters: transmission time in Real POS protocol

| *Message* | | *Data (bytes)* | *Packet length L (bytes)* | *ACL packets* $N_{DH5}$ | *Slots* $S_T$ | $T_T$ *(s)* | *Whole time* |
|---|---|---|---|---|---|---|---|
| 1 | Inq_p and Pag_s | – | – | – | – | 1.35 | |
| 2 | C to M | 500 | 556 | 2 | 11 | 0.0088 | |
| 3 | M to C | 7,920 | 7,976 | 24 | 143 | 0.0993 | |
| 4 | C to M | 6,684 | 6,740 | 20 | 119 | 0.0823 | 1.628 |
| 5 | M to C | 1,320 | 1,376 | 5 | 29 | 0.0201 | |
| 6 | C to TTP | 3,480 | 3,536 | 11 | 65 | 0.0466 | |
| 7 | TTP to C | 312 | 368 | 2 | 11 | 0.0088 | |
| 8 | C to M | 716 | 772 | 3 | 17 | 0.0126 | |

**Table 5** Parameters: transmission time in anonymous payment protocol

| *Message* | | *Data (bytes)* | *Packet length L (bytes)* | *ACL packets* $N_{DH5}$ | *Slots* $S_T$ | $T_T$ *(s)* | *Whole time (s)* |
|---|---|---|---|---|---|---|---|
| 1 | Inq_p and Pag_s | – | – | – | – | 1.35 | |
| 2 | C to M | 256 | 312 | 1 | 5 | 0.0051 | |
| 3 | M to C | 256 | 312 | 1 | 5 | 0.0051 | |
| 4 | C to M | 1,624 | 1,680 | 5 | 29 | 0.0201 | 1.410 |
| 5 | M to TTP | 1,064 | 1,120 | 4 | 23 | 0.0163 | |
| 6 | TTP to M | 560 | 616 | 2 | 11 | 0.0088 | |
| 7 | M to C | 280 | 336 | 1 | 5 | 0.0051 | |

**Table 6** Parameters: transmission time in KSL protocol

| *Message* | | *Data (bytes)* | *Packet length L (bytes)* | *ACL packets* $N_{DH5}$ | *Slots* $S_T$ | $T_T$ *(s)* | *Whole time (s)* |
|---|---|---|---|---|---|---|---|
| 1 | Inq_p and Pag_s | – | – | – | – | 1.35 | |
| 2 | C to M | 2,500 | 2,556 | 8 | 47 | 0.0333 | |
| 3 | M to C | 1,000 | 1,056 | 4 | 23 | 0.0163 | |
| 4 | C to M | 4,044 | 4,100 | 13 | 77 | 0.0541 | |
| 5 | M to TTP | 4,320 | 4,376 | 13 | 77 | 0.0541 | 1.620 |
| 6 | TTP to I | 4,320 | 4,376 | 13 | 77 | 0.0541 | |
| 7 | TTP to A | 1,000 | 1,056 | 4 | 23 | 0.0163 | |
| 8 | I, A to TTP | 660 | 716 | 3 | 17 | 0.0126 | |
| 9 | TTP to M | 1,320 | 1,376 | 5 | 29 | 0.0201 | |
| 10 | M to C | 600 | 656 | 2 | 11 | 0.0088 | |

**Table 7** Parameters: transmission time in M-cash protocol

| | *Message* | *Data (bytes)* | *Packet length L (bytes)* | *ACL packets* $N_{DH5}$ | *Slots* $S_T$ | $T_T$ *(s)* | *Whole time (s)* |
|---|---|---|---|---|---|---|---|
| 1 | Inq_p and Pag_s | – | – | – | – | 1.35 | |
| 2 | C to M | 6,100 | 6,156 | 19 | 113 | 0.0786 | |
| 3 | M to C | 6,600 | 6,656 | 20 | 119 | 0.0823 | |
| 4 | C to M | 208 | 264 | 1 | 5 | 0.0051 | |
| 5 | M to C | 2,000 | 2,056 | 7 | 41 | 0.0296 | 1.637 |
| 6 | C to M | 2,064 | 2,120 | 7 | 41 | 0.0296 | |
| 7 | M to TTP | 2,924 | 2,980 | 9 | 53 | 0.0371 | |
| 8 | TTP to M | 660 | 716 | 3 | 17 | 0.0126 | |
| 9 | M to C | 660 | 716 | 3 | 17 | 0.0126 | |

## 7.2 Computational cost evaluation

In this sub-section, we determine the number of cryptographic operations carried out in each payment protocol and calculate their computational cost.

Table 8 shows the number of cryptographic operations carried out by each entity in the five mobile payment protocols. However, the operations of authentication using certificates where not included, since they depend on the scenario.

**Table 8** Cryptographic operations performed by each entity during the payment protocol

| | *Virtual POS* | | | *Real POS* | | | *Anonymous* | | | *KSL* | | | *M-cash* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *OP* | *C* | *M* | *TTP* | *C* | *M* | *TTP* | *C* | *M* | *TTP* | *C* | *M* | *TTP* | *C* | *M* | *TTP* |
| $OP_{ENC}$ | 1 | 1 | 0 | 2 | 0 | 0 | 2 | 3 | 2 | 0 | 1 | 1 | 1 | 0 | 0 |
| $OP_{DEC}$ | 0 | 1 | 1 | 0 | 1 | 1 | 2 | 2 | 2 | 0 | 1 | 1 | 0 | 2 | 2 |
| $OP_{SIG}$ | 2 | 1 | 1 | 3 | 2 | 1 | 2 | 3 | 2 | 0 | 1 | 1 | 0 | 0 | 0 |
| $OP_{VER}$ | 1 | 2 | 2 | 3 | 2 | 2 | 1 | 2 | 2 | 0 | 1 | 1 | 0 | 0 | 0 |
| $OP_{SYM}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 4 | 0 | 4 | 6 | 2 |
| $OP_{HASH}$ | 5 | 5 | 6 | 6 | 4 | 3 | 2 | 2 | 3 | 3 | 3 | 0 | 0 | 1 | 1 |

When the customer C carries out the authentication protocol with the merchant M, it must verify the certification path of M and the merchant verifies the certification path of C. In the scenario described in Section 6 (Figure 3), the customer and merchant must obtain the certificate of the CCCA, the TTP and the user that are part of the path, so they carry out three hash and three signature verification operations during the path validation process.

Table 9 shows the total number of cryptographic operations including the operations related with the authentication process carried out by each entity in three different mobile payment protocols. We do not include anonymous payment and KSL protocols, since these protocols do not carry out an authentication process using certificates.

**Table 9** Cryptographic operations performed by the customer, merchant and TTP

| | *Virtual POS* | | | *Real POS* | | | *M-cash* | | |
|---|---|---|---|---|---|---|---|---|---|
| *Operation* | *C* | *M* | *TTP* | *C* | *M* | *TTP* | *C* | *M* | *TTP* |
| $OP_{ENC}$ | 1 | 1 | 0 | 2 | 0 | 0 | 1 | 0 | 0 |
| $OP_{DEC}$ | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 2 | 2 |
| $OP_{SIG}$ | 2 | 1 | 1 | 3 | 2 | 1 | 0 | 0 | 0 |
| $OP_{VER}$ | 4 | 5 | 2 | 6 | 5 | 2 | 3 | 3 | 0 |
| $OP_{SYM}$ | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 6 | 2 |
| $OP_{HASH}$ | 8 | 8 | 6 | 9 | 7 | 3 | 3 | 4 | 1 |

Equation (5) is used to calculate the computational cost (COST) of cryptographic operations carried out by the customer, merchant and trusted third parties in the different mobile payment protocols. The numbers of encryption/decryption operations are denoted with $OP_{ENC}$ and $OP_{DEC}$, the number of signature creation/verification operations with $OP_{SIG}$ and $OP_{VER}$, the number of symmetric key encryption/decryption operations with

$OP_{SYM}$ and the number of hash operations with $OP_{HASH}$. The execution time of each operation is defined with $T_X$ where $X$ denotes the operation.

$$COST = (OP_{ENC} * T_{ENC}) + (OP_{DEC} * T_{DEC}) + (OP_{SIG} * T_{SIG}) + (OP_{VER} * T_{VER}) + (OP_{SYM} * T_{SYM}) + (OP_{HASH} * T_{HASH}) \quad (5)$$

We assume that the customer and merchant use PDAs as mobile devices and TTPs (e.g., bank or payment gateway) use laptops. The analysis was performed using a PDA with a 200 MHz ARM920T processor and 64 MB, running Linux 2.4 operating system. The laptop has an 800 MHZ AMD Turion processor and 2 GB, running Linux. In both cases, we use RSA keys of 1,024 bits.

For the implementation of the cryptographic operations in the PDA, we employ Python 2.4 with Crypto library. The execution times obtained are: encryption/decryption operations performed using RSA algorithm take 0.0263s and 1.8990s, respectively; a signature creation requires 1.8973s and signature verification requires 0.0263s; encryption/decryption operations using DES algorithm take 0.0010s. We use SHA-2 as hash function and its execution time is 0.0006s.

In the laptop, the execution time obtained for encryption/decryption operations using RSA algorithm is 0.0004s and 0.0036s, and the execution time of signature creation/verification operations is 0.0014s and 0.0004s, respectively. The encryption/decryption operations using DES algorithm requires 0.00001s. We use SHA-2 as hash function and its execution time is 0.00001s.

Table 10 shows the computational cost of each entity with and without authentication.

**Table 10** Computational cost

| | | *COST (s)* | |
|---|---|---|---|
| *Protocol* | *Entity* | *Without authentication* | *With authentication* |
| Virtual POS | C | 3.850 | 3.93 |
| | M | 3.878 | 3.958 |
| | TTP | 0.005 | 0.005 |
| Real POS | C | 5.827 | 5.9 |
| | M | 5.748 | 5.829 |
| | TTP | 0.005 | 0.005 |
| Anonymous payment | C | 7.672 | – |
| | M | 9.622 | – |
| | TTP | 0.011 | – |
| KSL | C | 0.004 | – |
| | M | 3.829 | – |
| | TTP | 0.444 | – |
| M-cash | C | 0.03 | 0.111 |
| | M | 3.804 | 3.885 |
| | TTP | 0.007 | 0.007 |

### 7.3 Whole execution time

Figure 5 shows the whole execution time of each protocol. Finally, Figure 6 shows the whole execution time of three mobile payment protocols with and without performs the authentication process.

**Figure 5** Whole execution time: whole transmission time + COST

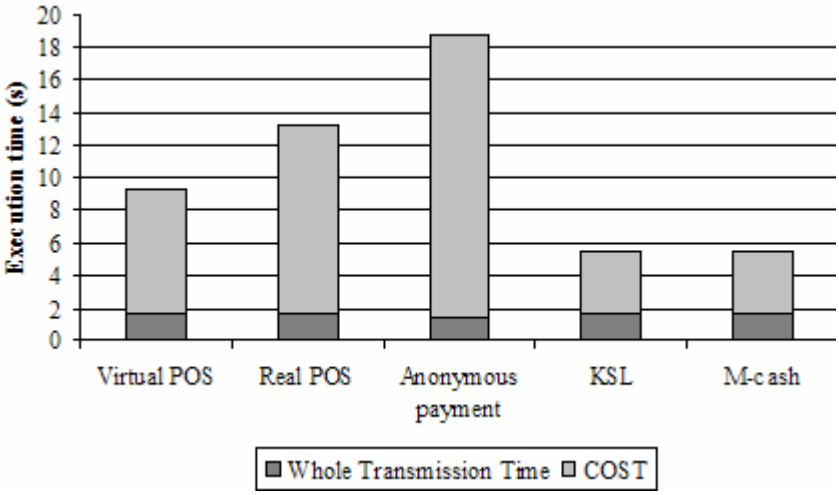
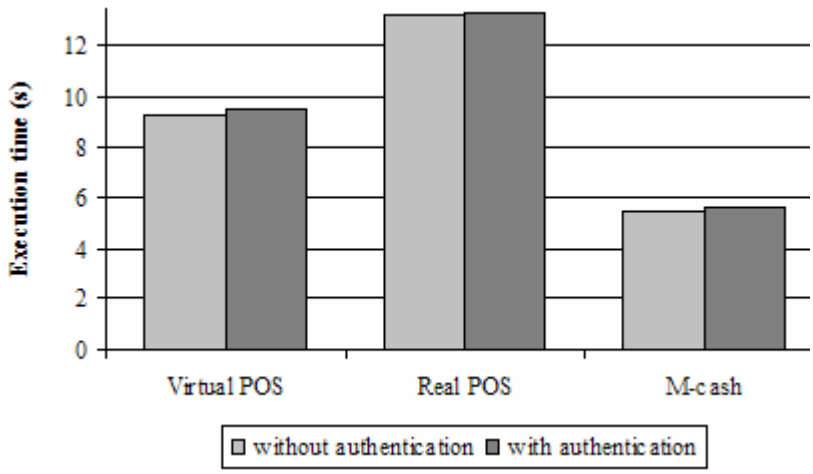



**Figure 6** Comparison of whole execution time




## 8 Conclusions

Mobile payment protocols are becoming more and more important in the new information technology as an alternative payment mechanism in many scenarios. The benefits of these protocols include simplicity of use, flexibility, comfort and mobility.

In this paper, we performed the evaluation of five mobile payment protocols with different characteristics. The calculation of the computational cost and the transmission time are key issues to determine its feasibility and success.

As shown in Table 10, the computational cost for each mobile payment protocol is acceptable in terms of the relation between security and performance; this means that, with more security (performing more cryptographic operations) the device requires more resources. Figure 5 shows the enormous difference among the protocols that perform symmetric key operations and the protocols that carry out only public key operations. Although the computational cost of asymmetric operations is higher than symmetric operations, its performance is suitable for new mobile devices, for example, the anonymous payment protocol requires less than 20s to complete all the process. On the other hand, the use of symmetric keys requires more storage capacity and has limitations when the entities require establishing a secure channel between unknown entities. PKI and certificates can resolve the problem caused by the use of symmetric keys between unknown entities providing secure authentication with acceptable performance as shown in Figure 6.

## Acknowledgements

This work has been supported in part by the Spanish public funded projects ARES (CONSOLIDERINGENIO-2010 CSD2007-00004) and ITACA (TSI2006-13409-C02-02) and graduate scholarship from CONACYT (Mexico). We are thankful to the reviewers for their constructive, critical and helpful comments, which helped improve this manuscript. Moreover, we wish to thank Guillermo Díaz, Jhon Padilla, Juan Vera, Rafael Páez and Alfredo Abad.

## References

Argyroudis, P.G., Verma, R., Tewari, H. and O'Mahony, D. (2004) 'Performance analysis of cryptographic protocols on handheld devices', *Proceedings of the IEEE International Symposium on Network Computing and Applications, (NCA'04)*, pp.169–174.

Bruno, R., Conti, M. and Gregori, E. (2002) 'Bluetooth: architecture, protocols and scheduling algorithms', *Cluster Computing*, Vol. 5, pp.117–131.

Choi, Y.B., Crowgey, R.L., Price, J.M. and VanPelt, J.S. (2006) 'The state-of-the-art of mobile payment architecture and emerging issues', *International Journal of Electronic Finance*, Vol. 1, pp.94–103.

Das, M.L., Saxena, A. and Gulati, V.P. (2005) 'A security framework for mobile-to-mobile payment network', *Proceedings of the IEEE International Conference on Personal Wireless Communications, (ICPWC 2005)*, pp.420–423.

Delic, N. and Vukasinovic, A. (2006) 'Mobile payment solution – symbiosis between banks, application service providers and mobile network operators', *Proceedings of the International Conference on Information Technology: New Generations (ITNG'06)*, pp.346–350.

Ferro, E. and Potorti, F. (2005) 'Bluetooth and Wi-Fi wireless protocols: a survey and a comparison', *IEEE Wireless Communications*, Vol. 12, pp.12–26.

Gao, J., Edunuru, K., Cai, J. and Shim, S. (2005) 'P2P-paid: a peer-to-peer wireless payment system', *Proceedings of the IEEE International Workshop on Mobile Commerce and Services (WMCS'05)*, pp.102–111.

Hassinen, M., Hyppönen, K. and Haataja, K. (2006) 'An open, PKI-based mobile payment system', *Proceedings of the International Conference on Emerging Trends in Information and Communication Security (ETRICS'06)*, pp.86–100.

Heijden, H.V.D. (2002) 'Factors affecting the successful introduction of mobile payment system', *Proceedings of the Bled Electronic Commerce Conference eReality: Constructing the eEconomy*, pp.430–443.

Houseley, R., Polk, W.T., Ford, W. and Solo, D. (1999) *Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459*, pp.1–129.

Isaac, J.T., Camara, J.S., Manzanares, A.I. and Marquez, J.T. (2006) 'Anonymous payment in a kiosk centrik model using digital signature scheme with message recovery and low computational power device', *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 1, pp.1–11.

Johansson, N., Kihl, M. and Körner, U. (2000) 'TCP/IP over the Bluetooth wireless ad-hoc network', *Proceedings of the IFIP-TC6 / European Commission International Conference on Broadband Communications, High Performance Networking, and Performance of Communication Networks*, pp.799–810.

Kungpisdan, S., Srinivasan, B. and Le, P.D. (2003) 'Lightweight mobile credit-card payment protocol', *Proceedings of the International Conference on Cryptology in India, Progress in Cryptology*, INDOCRYPT, LNCS 2904, pp.295–308.

Martínez Peláez, R. and Rico Novella, F.J. (2006) 'Application of electronic currency on the online payment system like PayPal', *Proceedings of the IFIP Conference on E-Commerce, E-Business and E-Government, (I3E 2006)*, Vol. 226, pp.44–56.

Martínez-Peláez, R. and Rico-Novella, F.J. (2006a) 'New electronic cash model: a script anonym', *Proceedings of the IADIS International Conference on E-commerce, (e-commerce'06)*, pp.392–396.

Martínez-Peláez, R., Satizabal, C., Rico-Novella, F. and Forné, J. (2008) 'Efficient certificate path validation and its application in mobile payment protocols', *Proceedings of the International Workshop on Frontiers in Availability, Reliability and Security, (FARES'08)*, pp.701–708.

Nambiar, S., Lu, C-T. and Liang, L-R. (2004) 'Analysis of payment transaction security in mobile commerce', *Proceedings of the IEEE International Conference on Information Reuse and Integration, (IRI'04)*, pp.475–480.

Panurach, P. (1996) 'Money in electronic commerce: digital cash, electronic fund transfer and Ecash', *Communications of the ACM*, Vol. 39, pp.45–50.

Satizábal, C., Martínez-Peláez, R., Forné, J. and Rico-Novella, F. (2007a) 'Reducing the computational cost of certification path validation in mobile payment', *Proceedings of the European PKI Workshop, (EuroPKI'07)*, pp.280–296.

Satizábal, C., Paez, R. and Forne, J. (2007b) 'WAP PKI and certification path validation', *International Journal of Internet Protocol Technology*, Vol. 2, pp.88–95.

Shon, T.H. and Swatman, P. (1998) 'Identifying effectiveness criteria for internet payment systems', *Internet Research*, Vol. 8, pp.202–218.

Tillich, S. and Grobschädl, J. (2004) 'A survey of public-key cryptography on J2ME-enabled mobile devices', *Proceedings of the International Symposium on Computer an Information Sciences, (ISCIS'04)*, pp.935–944.

WAPforum (2001) 'WAP certificate and CRL profiles, specification WAP-211-WAPCert-20010522-a', pp.1–32.

WAPForum (2001a) 'Wireless application protocol public key infrastructure specification', WAP-210-WAPArch-20010712-a.

WAPForum (2001b) 'Wireless transport layer security, specification WAP-261-WTLS-20010406-a'.

Wrona, K., Schuba, M. and Zavagli, G. (2001) 'Mobile payments – state of the art and open problems', *Proceeding of the International Workshop on Electronic Commerce, (WELCOM'01)*, pp.88–100.