46

Mobile Payment Solutions

Martin Gerdes and Dr. Silke Holtmanns
Ericsson Eurolab Deutschland GmbH, Research Department

Abstract: Mobile telecommunication has become a pillar of the everyday communication both in global business and society. The number of people using mobile devices is growing rapidly. New protocols and technologies like WAP, GPRS and UMTS enable powerful applications and the expansion of the known Internet towards a Mobile Internet. New mobile services and applications emerge that require payment methods for information, goods or the service itself. For payments involving a mobile phone special restrictions have to be taken into account. An investigation of selected existing mobile payment solutions under consideration of security risks and possible improvements will be presented, concluded by a comparison of used security mechanisms.

1. INTRODUCTION

To investigate the security of selected mobile payment systems we start with a general background on the development of M-commerce. In the next section we state the performance and hardware constraints of the mobile environment. Here we also compare the security methods for wired Internet and mobile environments. With this technical knowledge we can review the different mobile payment systems under consideration of the following aspects:

- Payment scenario (since electronic transactions in principle pose a higher risk than POS transactions).
- Message flow between the parties.
- Analysis of the message flow with regard to used security methods.
- Discussion of possible attacks.

Based on this data we point out improvement possibilities. If available we added privacy information. We close by summarizing the security methods used in a comparative table. It has to be noted that the developing companies tend not to give away detailed information of their payment systems.

2. DEVELOPMENT OF M-COMMERCE

The rate of mobile phone penetration has reached and even overtook the highest reaching expectations of several industry observers (see *Table 5*)

Table 5. Worldwide Mobile Cellular Subscriber Forecasts (in million subscriber)

	2000	2003	2005	2010
UMTS Report 8 (1997)	426		941	1700
Robertson Stephens (2000)	600	795	1735	
DLJ (2000)	600	1200		
Merill Lynch (2000)	500	1200	1400	2250
Strategis (1999)	503	795	915	
EMC (2000)	633	1151		

Sources: Merill Lynch, Strategis, DLJ, EMC, UMTS Forum Robertson Stephens.

Fact is that at the end of 2000 about 700 million world cellular mobile subscribers exist [EMC]. In Germany alone the number of subscribers of each D2 Vodafone and D1 T-Mobile doubled in less than one year and both reached 20 millions in February 2001. Together with the 1800MMz E-networks this led to about 50 million GSM customers in Germany (the trend to multiple subscriptions is not taken into account).

The main application currently used is voice, but that has started to shift. In Europe the amount of SMS has increased rapidly and many operators make substantial parts of their revenue on that service. E.g. Nordic operators are reporting 7 – 10 % of their revenue is due to SMS traffic. At the end of 1999 10 SMS were sent per GSM subscriber per month, at the end of 2000 it have been 30 (Source: EMC World Cellular Database).

The expectations to the "Mobile Internet" are very high, but still the development of suitable applications, and also feasible mobile devices takes a while. Therefore it is not that surprising that headlines like "WAP is dead" are distributed. New devices will have much more performance and user-friendliness (color display, organizer functionality like calendar tool, address book and notepad, e-mail, WAP and HTML browser). In addition broader bandwidth and the easy access everywhere will push m-commerce forward.

3. PERFORMANCE FEATURES AS LIMITING FACTORS

To compare different payment methods the capabilities of the used hardware platforms and underlying transmission services have to be taken into account. Major impacts in this context have the transmission delay of the used communication service and the hardware resources of the relevant device.

3.1 Transmission bandwidth and delay

Depending on the payment method a varying number of messages containing different amounts of information have to be exchanged between the payment peers. In case of (relatively) large amount of information the transmission bandwidth has to be considered, while in case of small messages just the transmission delay and hence the Round Trip Time (RTT) of the connection has an influence. When for example digital certificates are used to authenticate the origin of the signatures of payment messages these messages reach a size of about 18 Kbytes what would result in a pure transmission time of about 16 seconds in today's GSM networks. In general the single messages exchanged for initiation of payments and payee authentication are relatively small and only the transmission delay has to be examined. The following table gives an overview over these characteristics.

Table 6. Transmission characteristics

Transmission service	Data rate	Transmission delay (RTT)
(Fixed) Internet (LAN / Modem)	100kBit/s – 1 MBit/s/ 50 kBit/s	Depending on network AND server load: ~50ms
GSM (WAP over data bearer)	~ 9kEit/s	~ 750ms
GSM (SMS)	160Bytes/message	> 5s (unpredictable)
GPRS	~20kBit/s	~ 1s
UMTS (outdoor)[62]	~ 100kBit/s	~ 500ms
UMTS (indoor)[62]	~ 1Mbit/s	~ 250ms

3.2 Hardware resources

When it comes to the implementation of payment services, security issues of the transmitted payment data (i.e. user data and payment details) have to be considered. Security in telecommunication networks requires cryptographic functions. Depending on the cryptographic method and implementation used to encrypt the data that have to be transmitted over insecure links (and to decrypt received messages) the following hardware limitations have to be considered:

- Memory requirements for the additional function implementation itself as well as temporary memory required during the encryption operation.
- Processing load, due to execution of the additional protocol, but even more due to the cryptographic computation functions.

[62] The UMTS radio access networks will use different technologies for outdoor (i.e. open space) and indoor (i.e. within buildings, airports, stations etc.) installations. They differ significantly in the available data rates on the one hand, but also on the provided radio access range on the other hand.

3.3 Security mechanisms

Figure 4 gives an overview over the whole end-to-end M-commerce scenario (with a simplification on the payment side where in fact more parties are involved, depending on the used payment system). In particular it shows physical connections, which are possible targets of fraudulent access or third party tapping.

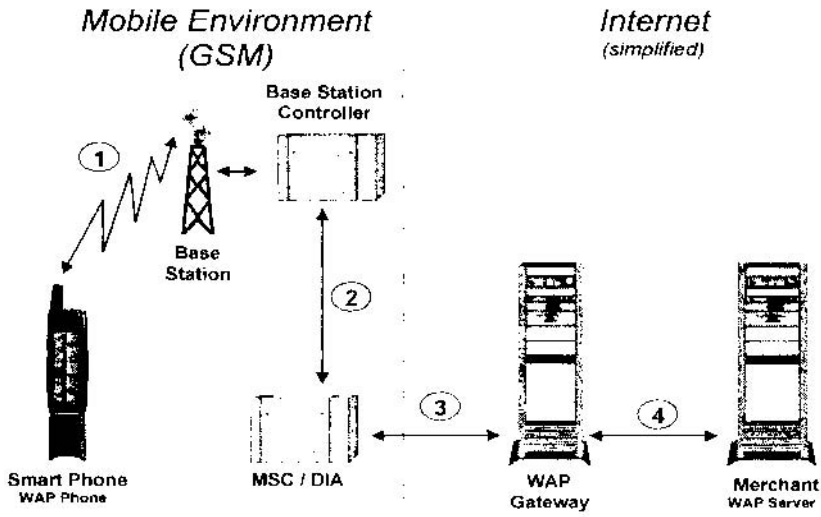

Figure 4. M-commerce scenario

Within the *Internet* the following security and privacy protection mechanisms are provided:

3.3.1 SSL (Secure Socket Layer) (connection (3) and (4)):

SSL has been developed by Netscape. It was designed to provide public key security for secure transactions between browser and servers. The SSL protocol can be found in many hard- and software based security products. SSL uses the PKCS.

3.3.2 TLS (Transport Layer Security) (connection (3) and (4)):

The TLS protocol is a proposed IETF standard that provides security features at the transport layer. TLS is based on SSL 3.0. Additionally TLS offers options for authentication. Three levels of server security include server verification by using digital certificate, encrypted data transmission and verification that the integrity of

an arrived message (i.e. the content has not been manipulated during transfer) is given.

In the *mobile environment* the following security mechanisms are available:

3.3.3 GSM radio path ciphering:

A radio access network comprises inherently a higher risk for fraudulent access then a fixed (wired) network. Hence mechanisms for data encryption on the radio path (connection (1) in *Figure 4*), in particular of subscriber data are of high importance. The GSM standard foresees the possibility of radio path ciphering, especially ciphering of all subscriber information transmitted during the authentication phase, to prevent third party tapping. It has to be mentioned that the radio path ciphering is up to the network operator and cannot be influenced by the subscriber. Furthermore, within the wired infrastructure (i.e. the core network, connection (2) in *Figure 4*) of a mobile communication system, all transmissions are performed in clear text, as they are in a PSTN network. This applies in particular to the short message service SMS.

3.3.4 GSM subscriber data security

To prevent unregistered users from accessing a GSM network each subscriber has to authenticate himself using the subscriber identity module SIM. The subscriber identity is protected during the authentication process to prevent subscriber location disclosure. In fact the SIM is authenticated and not the subscriber. The SIM module and the authentication process involving the SIM are designed to protect the data it contains in two ways: it is not possible to read the SIM information once and use a mobile device without the physical SIM afterwards just with the information and only the SIM issuer can copy a SIM.

The authentication process is carried out between the SIM (plugged into a mobile device) and the home location register HLR (a central node within the GSM infrastructure where all subscriber data are stored). Therefore it is not possible to "simulate" a base station to get fraudulent access to subscriber data.

3.3.5 WIM (Wireless Identity Module):

The WIM is a tamper resistant device. It is used in performing WTLS and application level security functions, especially for storing and processing information needed for user identification and authentication. The WIM is designed for storing sensible data like keys or certificates. All operations that involve these keys can be performed by the WIM, then for example signing using a private key

could not be observed from outside the WIM. An example of a WIM implementition is the SIM card in a mobile phone.

3.3.6 WTLS (Wireless Transport Layer Security):

WTLS in a security layer protocol in the WAP architecture. It operates above the transport layer protocol (end-to-end, connection (1)-(4)). It provides the upper-level layer of WAP with a secure transport service interface that preserves the transport service interface below it. WTLS is modular and depends on the chosen security level of the given application. WTLS is designed for protecting privacy, data integrity and authentication between two communicating parties. WTLS has a similar functionality as TLS 1.0 and provides several new features like optimized handshake, dynamic key retieshing etc.

4. EXISTING MOBILE PAYMENT SOLUTIONS

We will now discuss the latest existing mobile payment solutions (February, 2001). GiSMo, Jalda, Mint, Net900, Paybox, Sonera Mobile Pay and TopUp will be discussed.

4.1 GiSMo

GiSMo is an Internet payment system available in the UK, Sweden and Germany and owned by Millicom International Cellular SA. It was developed in 1999 and concentrates in the moment mainly to Sweden. Countries like France, Netherlands, Belgium, Denmark, Austria, Finland, Luxembourg and Norway are intended for the future.

Following the user scenario a customer buys goods from an Internet service or content provider and the payment is authorized using a CSM-phone. The settlement of the amount is done by the payment service provider GiSMo. A customer has to apply for a GiSMo account. This procedure is very similar to a credit card application. E.g. the amount that could be spent within a month has also an upper limit, depending on the outeome of a financial research. The customer is billed monthly via e-mail. The system works as follows:

1. The customer wants to buy a good or service in an Internet Shop and chooses payment with GiSMo.
2. The customer sends a “Request order form” to the merchant’s server.
3. The merchant then sends the order form back to the customer (“Display order form”) via Internet.
4. The customer submits the order to the GiSMo server with his GiSMo account number.

5. GiSMo retums a PIN Code via the GSM network to the mobile phone of the customer.
6. The customer confirms the transaction by inserting the FIN into a field on the webpage and sends it to the GiSMo server.
7. GiSMo sends a digital receipt to the customer
8. GiSMo settles the account with the merchant.

The security concept is based on the assumption that for a fraud the GiSMo account number and the transaction PIN would be needed. Now we will study if and how this data is protected during the transmission:

– The Internet transfer is not secured by SSL or some additional encryption, hence someone could "listen" to get the GiSMo account number.
– Since no authentication of GiSMo-server is done, some other entity could pose as GiSMo and obtains this way the GiSMo account number.
– A person with a stolen phone and GiSMo account number would have no problem to pose as the "real'" customer, since no on-line customer authentication or signing is done.
– The mobile communication security relies only on the GSM network security. As the GSM ciphering only covers the radio path all messages can easily be tapped as soon as they leave the mobile network infrastructure towards the Internet.
– The user authentication uses only the SIM-card, hence only the GSM subscriber could be identified (assuming no stolen SIM) but not the GiSMo account owner.

Therefore a *possible attack* could be:

An attacker listens to the Internet traffic to capture the account number and then he steals the phone. Then the attacker can shop and is afterwards able to pose as the user by inserting the GiSMo account number and authorize the payment using the stolen phone. The argument that a delivery address ensures that the goods reach the right destination does not really work since the goods can also be off digital nature.

Compared to a non-SET (SET is a secure credit card payment system for Internet systems and was developed by Visa and MasterCard) secured credit card transaction the GiSMo payment system has the advantage that the merchant does not obtain the GiSMo account number, Even if he does he still needs the phone. Therefore fraud is not that easy for the merchant,

Concerning privacy GiSMs probably can collect personal: shopping data to build a personal user profile.

With appropriately added encryption, authentication, certificates and PKI this system maybe useful.

4.2 Jalda

Jalda is a development of EHPT. EHPT is a software vendor for telecom operators as well as Internet service providers and is jointly owned by Ericsson and Hewlett-Packard. Jalda is designed for payments made for Internet shopping. The settlement could be done via operator bill, electricity bill or cable TV bill depending on the customer this payment system is installed for. For example Telia, Sweden's largest telecom operator, uses Jalda in their online payment solution. A credit card interface can also be added. Jalda is an API that can be integrated in other payment solutions like Mobile e-Pay. We describe now the message flow of Mobile e-Pay, which founds on Jalda. There also exists a pre-paid card system solution, where a PIN on a card is revealed by scratching and by entering this PIN on the website the account is activated. The Jalda pre-paid card payment solution is currently just available in the UK. In the rest of Europe the rollout will not be started before 2002.

1. The customer chooses to buy a good (digital or solid) from an ISP and payment via Jalda.
2. The ISP receives an order.
3. The ISP sends a payment request to the payment provider using Jalda.
4. The payment provider sends a digital contract via the ISP to the end users mobile phone with a password request as a SMS.
5. The end user accepts the contract and confirms the payment by entering a password, which is sent with SMS back to the Mobile e-Pay server.
6. The Mobile e-Pay server then validates the password.
7. The Mobile e-Pay server generates a digital signature in PKCS#7 format, which acts as the signed contract.
8. The Jalda payment server then verifies the signed digital contract.
9. The Jalda Payment server sends an ok after approval to the ISP.
10. The Jalda Payment server sends a receipt to the mobile phone of the end user.

The security is based on a two-zone security scheme. It consists of GSM encryption in the mobile network for sending the SMS in step 4 and 5. In the IP-based network PKI (RSA signing) and SSL-encryption is used. WPKI based security involving a password for end-user authentication to support application level security can be added.

This payment system is designed to reach most of the mobile phones on the market with highest possible security. The security add-on like WPKI are in the moment only supported by a small number of phones. Also WTLS should be integrated into future releases of this payment system to secure the "over the air" transmission on the transport layer. The possibility that future phones will be able to store RSA keys and perform signatures should also be exploited.

The merchant does not obtain any sensitive data, but it is unclear how much data the Jalda payment server and the Mobile e-Pay server can collect. More information about the exact data field transmitted is necessary to answer that question. A

possibility for the user to choose her privacy policy would be a good addition to this system.

4.3 Mint

Mint is a POS payment system of Mint AB. In the moment (February 2001) it is available in Stockholm, Sweden. The merchants have to be equipped with a special Mint payment terminal. The customer has to register to Mint as a MintCash (MintKontaktkund) or a MintCredit (MintKreditKund) user. A MintCash customer deposits the amount she wishes into a postgirokonto (post bank account) and obtains later an activation letter by mail. A MintCredit customer has to pay after receiving a monthly invoice. The upper limit is 5000 Swedish crowns per month. A payment transaction using either of both systems includes the following steps.

1. The merchant enters the amount of the purchase into the Mint payment terminal.
2. The Mint payment terminal displays a telephone number (terminal specific number).
3. The customer dials this number.
4. If the amount exceeds the predefined limit, the user has to enter his PIN, if it is lower the customer just accepts.
5. The merchant obtains “payment accepted” or “payment failed” on the payment terminal.
6. The customer obtains a receipt-SMS and / or e-mail (the receipt is not an integral part of the payment transaction).
7. Mint settles the accounts.

The first communication between the customer’s phone and the Mint computer system is secured by the GSM security. The identification of the customer is based on the SIM authentication during the phone call in step 3 and 4.

The second communication is between the merchant’s Mint payment terminal and the Mint computer system. This communication link is encrypted (not clear which method is used). Over this link the payment amount, “payment accepted” and “payment failed” messages. Mint claims that the PIN code control is also handled over this communication (but since the PIN is inserted by the customer and send to the Mint computer system it is unclear how the connection between the merchant and the Mint computer system corresponds to this).

Another communication is using the Internet. Here merchant and customer can access their payment information and only that. This communication is also secured, but the method (probably SSL) is unclear.

The main risk is that someone steals or finds a lost mobile phone. This person could make payments below the PIN entry level (note that can be several payments which sum up over the specified PIN entry level) until Mint blocks the account. But if someone looks over the shoulder during PIN insertion and steals then the phone

the damage caused could be very serious. The customer has the option to specify the amount for which a PIN authorization is necessary.

Another security risk could be the link between the merchant and the Mint payment terminal, since it is not clear how it is secured. If for example someone is paying for something very expensive and manage to replace the message "payment failed" by "payment accepted" the system has a major drawback.

The privacy policy of Mint states:

"For marketing purpose the information will be used to give the customer relevant offers and information reflecting those areas of interests that the customer might have registered with Mint."

In other words: They will profile the user and use this personal user profile for marketing purposes like advertisements from Mint.

"Mint will make it possible for retailers and advertisers to send targeted information to the customer via SMS, e-mail, fax or mail", but here the customer can choose the subject area, interests and other conditions for the information, offers and services that she wants to receive. Also the customer can state how and when the information and specific services are to be delivered. Therefore the customer could block unwanted advertisements from other companies.

The customer is anonymous to the merchant.

4.4 Net900

Net900classic is an operator centric micropayment solution for digital goods like software, videos, and music that can be downloaded in the Internet. The Kontopass Net900 shall replace the Net900 classic solution very soon. The Kontopass Net900 solution is bank account based. Both have been developed by In Medias Res, which has a close relationship with the Deutsche Telekom AG. Net900 started in April 2000. The payment system is in the moment restricted to Germany, but there are plans to include the whole EU, Norway and Switzerland till the end of 2001. Many service providers support that system (AOL, Compuserve, Comundo, Germany.net, MobilCom, Freenet, T-Online). The customer is charged on the monthly operator bill or on the bank account of the user.

The user has to install special software on his PC. During the installation bank account, bank name and user name has to be provided. This data is send to Net900 secured via SSL-secured Internet connection. Net900 sends than a money order (EFT) to the bank account and provides the secret PIN in the subject. By inserting the PIN the account is then activated and the user can start shopping (it is not clear if these session are also secured via SSL). The payment transactions are secured by an additional personal passphrase. How to set or to obtain this passphrase is unclear. Also where it has to be inserted (in an Internet interface or in the phone). No message flow protocol is available from In Medias Res. The PIN is probably only

used for activating the account (unclear if the account has to be activated only once or before every payment transaction) not for authentication or signing. There are probably the following weaknesses:

- If the user password is inserted in the Internet, the transfer of this password seems not to be secured by SSL or other means.
- No additional authentication of the user is done, so once the passphrase is "found" by an attacker, he can shop until the account is blocked.
- No authentication of Net900 is done, so someone could pose as a Net900 and got then the passphrase easily.
- User set passwords can be very weak for "uneducated users".
- If the password is inserted using a phone, security mechanisms are completely unclear.

The security situation here is similar to the one of GiSMo except that for registration purpose the session is SSL secured. Assumed that the passphrase is entered in the PC one has to observe that the authentication of the user is even weaker for Net900 than for GiSMo since the PC has no SIM card based authentication mechanism.

Privacy seemed not to be a design criterion for Net900, since this subject and / or the corresponding mechanisms are mentioned nowhere in their product description.

4.5 Paybox

Paybox is designed for several payment scenarios: Internet payments, Mobile to Mobile payments, Point of Sales payments. It is operational since May 2000. Deutsche Bank AG strongly supports Paybox.net AG. The customer is charged at her bank account. Since the POS scenario is the most used, we are only describing the message flow for this case:

1. The customer chooses the goods.
2. The customer gives the merchant his Paybox account number (not his telephone number).
3. The merchant calls a special number of Paybox and sends the amount and the customer's Paybox account number to Paybox.
4. Paybox calls then the customer and repeats the amount.
5. The customer inserts his Paybox PIN to authorize the payment.
6. Paybox settles the accounts.

For the online customer registration SSL is used. The Paybox PIN is only secured by the GSM standard network security. Authentication of the user is done via the SIM card. Due to the phone calls this system is not suitable for very small payments. In the case of Internet payments the merchant has also to phone Paybox and the user waits for the call from Paybox.

The system is designed to work on a large basis of existing mobile phones, therefore mechanisms like encryption, digital signatures and certificates are not

integrated in this system. The main security argument is that in the moment a large amount of Network traffic has to be captured and analysed before a Paybox PIN can be found. Even with a found Paybox PIN the mobile phone is needed. For the time being that is probably good enough. However, currently data transmitted between a mobile phone and the Paybox server is travelling in clear text through all fixed network parts, in particular the Paybox account PIN. This shows an existing security risk and should be solved with an end-to-end encryption mechanism.

4.6 Sonera Mobile Pay

Sonera Mobile Pay is a payment solution for soft-drink vending machines, shell car-wash, candy and snacks, video renting, parking machines, operator products and Internet purchases. The amount spent can be charged on the phone bill, bank account or credit card. The payment system is (currently) concentrated on Finland. The security of their payment system is developed in co-operation with SmartTrust Ltd. Since SmartTrust has several security solutions it is not clear which one is used. The information available is that the feature that a customer can authenticate a payment by inserting a 4-digit PIN is optional. The user is informed via SMS about the price.

4.7 TopUp

TopUp by SmartTrust [SmartTrust] is also an operator centric pre-paid mobile payment solution. Sonera SmartTrust Ltd is a complete subsidiary of Sonera Corporation [Sonera]. There exists an Internet and a mobile payment solution. The rollout has started in November 2000. The basic idea is that the customer can refill or "top-up" his prepaid account. The customer registers to TopUp where the customer identity and payment method (for example credit card number) is stored. This payment system is designed to add new e-commerce services later. The transaction for adding new value to the prepaid account runs as follows:

1. The top up process is initiated by selecting the service menu from the main menu on the phone.
2. The customer selects the desired amount.
3. The selection is then confirmed with a digital signature that is activated after entering a PIN (digitally signed SMS via 3DES).
4. When the top up request is signed it will be sent to the SmartTrust TopUp application. There it will be checked, if the digital key corresponds to the user identity.
5. The user's account is then credited.
6. The user receives a confirmation including the new balance.

During step 5 after authorization in step 4, the corresponding payment mechanism (e.g. credit card number) is retrieved from the payment method database.

A payment authorization request incl. name and payment method is prepared and submitted for authorization to the payment clearance gateway.

This database contains many very sensitive data and is likely to be a target for attacks.

From the privacy point of view, we would just like to state the following sentences from the SmartTrust webpages:

"Improved customer relationship: The convenience of the SmartTrust TopUp solution will motivate end users to register for the service. The prepaid customer will no longer be an anonymous one. SmartTrust TopUp provides the mobile operator with tools to profile the customer more accurately, by monitoring individual and collective spending habits."

5. CONCLUSIONS

Table 7. Comparison of security methods

Payment System	Security methods
GiSMo	GSM-encryption; PIN
Jalda	GSM-encryption; PIN; digital signature; SSL (WPKI, password can be added)
Mint	GSM-encryption; PIN; SSL
Net900	SSL (partial); PIN; passphrase
Paybox	GSM-encryption; PIN; call-back mechanism
Sonera Mobile Pay	GSM-encryption; PIN (optional)
TopUp	GSM-encryption; PIN; digital signature

There exist many good ideas and approaches for mobile payment applications, but the technical implementations are currently not as secure as they could be. Most mobile payment systems try to facilitate the use of "older" but widely distributed mobile phones to a high degree, though these phones are not provisioned with e.g. signing techniques and encryption procedures. It can be expected that the security of the payment systems increases according to the market share of phones able to support this. But the awareness concerning customer privacy develops very slowly.

6. ABBREVIATIONS

API	Application Programming Interface
DES	Data Encryption Standard
EFT	Electronic Fund Transfer
HLR	Home Location Register
HTML	Hypertext Mark-up Language
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
GSM	Global System for Mobile Communications
MSC / DIA:	Mobile Switching Center with Direct Internet Access
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standar
PKI	Public Key Infrastructure
POS	Point of Sales
PSTN	Public Switched Telephone Network
RSA	Rivest Shamir Adleman (Public key cryptosystem)
RTT	Round Trip Time
SET	Secure Electronic Transactions
SIM	Subscriber Identity Module
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications Systems
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WTLS	Wireless Transport Layer Security

7 . REFERENCES

[EHPT] http://www.ehpt.com/
[EMC] Market Intelligence for World Wireless Industry http://www.emc-database.com/
[GiSMo] http://www.GiSMo.net/
[GSM] The GSM System for Mobile Communications; M. Mouly, M.-B. Pautet; Cell & Sys, 1992
[IETF] Internet Engineering Task Force http://www.ietf.org/
[Jalda] http://www.jalda.com/
[Mint] http://www.mint.nu/
[Mobile Pay] Sonera Mobile Pay http://www.sonera.fi/english/solutions/mobilepay/
[Net900] http://www.in-medias-res.com/net900.htm
[Paybox] http://www.paybox.de
[SmartTrust] Sonera SmartTrust Ltd. http://www.smarttrust.com/
[Sonera] Sonera Corporation http://www.sonera.fi/english/
[TopUp] http://www.sonera.fi/; http://www.smarttrust.com
[UMTS] UMTS Forum http://www.umts-forum.org/
[WAP] WAP Forum http://www.wapforum.org/
[WPKI] Wireless Public Key Infrastructure http://www.wapforum.org/