SeMoPS: A Global Secure Mobile Payment Service

Stamatis Karnouskos [a], András Vilmos [b], Antonis Ramfos [c],
Balázs Csik [d], Petra Hoepner [a]

[a] Fraunhofer Institute FOKUS (www.fokus.fraunhofer.de)
Kaiserin Augusta Allee 31, D-10589, Berlin, Germany
Phone: +49-30-34637000, Fax: +49-30-34638000
email: {Stamatis.Karnouskos | Petra.Hoepner}@fokus.fraunhofer.de

[b] SafePay Systems Ltd (www.safepaysys.com)
Kapás u. 11-15, H-1027, Budapest, Hungary,
Phone: + 36-1-2124321, Fax: +36-1-2121122
email: vilmos@safepaysys.com

[c] Intrasoft International (www.intrasoft-intl.com)
19,7 Km Markopoulou Ave, GR-19002 Peania, Athens, Greece.
Phone: +30 210 6876482, Fax: +30 210 6876478
email: antonis.ramfos@intrasoft-intl.com

[d] ProfiTrade 90 Ltd (www.profitrade.hu)
25. Bécsi út, H-1023, Budapest, Hungary
Phone: +36-1-2357078, Fax number: +36-1-235706
email: balazs.csik@profitrade.hu

Abstract -- Many experts consider that efficient and effective mobile payment solutions will empower existing e- and m-commerce efforts and unleash the true potential of mobile business. Recently, different mobile payment approaches appear to the market addressing particular needs, but up to now no global mobile payment solution exists. SEMOPS is a secure mobile payment service with an innovative technology and business concept that aims to fully address the challenges the mobile payment domain poses and become a global mobile payment service. We present here a detailed description of the approach, its implementation, and features that diversify it from other systems. We discuss on its business model and try to predict its future impact. The aim is to provide an insight of a new mobile payment service and discuss on implementation decisions and scenarios.

INTRODUCTION

The increasingly popular ownership of mobile personal, programmable communication devices worldwide promises an extended use of them in the purchase of goods and services in the years to come (Mobey Forum, 2003). Security in payment transactions and user convenience are the two main motivations for using mobile devices for payments.

Authorisation in existing electronic payment systems, including ATM and credit/debit card transactions as well as on-line payments through a PC, is based on account-holder authentication. Account-holder authentication, however, can fail in multiple ways, of which the most usual is the case of the compromise of the user's computer, which is, typically, protected with minimal security mechanisms and processes. Moreover, existing payment networks do not always distinguish among user fraud, compromise of the user's computer, or compromise of the bank's computer. For example, in most countries, if the user claims not to have authorised a credit card transaction, the transaction has to be cancelled and the bank cannot prove that the user is not cheating. In such cases, responsibility is not necessarily allocated fairly, and non-corrupted, innocent parties may find themselves responsible for somebody else's fraudulent activity or security breach. The lack of a technical solution for preventing and resolving fraud creates substantial risk and expense for users, merchants and banks alike.

It is now well understood that a secure electronic payment transaction can only be ensured through a device that offers its own I/O interface to the user, so that the initiator of the payment transaction is clearly identifiable (Pfitzmann et al., 1999). Mobile personal devices provide a technical solution for personalised I/O interface to payment transactions since it can be safely assumed that the transaction initiator is in the majority of the cases also the owner of the mobile device. Security in payment transactions through a mobile device, therefore, is ensured by the authentication mechanisms of existing mobile devices, as a way to prevent call theft. Moreover, additional built-in mechanisms to ensure secure transaction authorisation and execution are relatively easy and inexpensive to be incorporated by device manufacturers. Therefore, payment through mobile devices benefits merchants and banks by supporting transactions where most fraud is prevented and responsibility for the remaining fraud is fairly allocated. As far as the end customer is concerned, the value of secure transactions far outweighs their possible cost.

Convenience is the other reason people are expected to use mobile personal devices for payments. Convenience can result from people using their mobile personal device when paying for goods and services, while on foot, in cars, planes, or trains, and when authorising payment transactions at remote servers of banks, brokerages, and merchants. Payments through mobile devices will enable validation of the customer's consent to the transaction during online, by telephone or by post purchases, since the merchant and the customer are at separate locations and the merchant cannot get the customer to sign in order to authorise the payment. In addition, payment through mobile devices will enable the secured purchase of content and services delivered via the network, as well as person-to-person payments and money transfer.

SEMOPS is a secure mobile payment service with an innovative technology and business concept (Karnouskos et al., 2003) that aims to fully address the challenges the mobile payment domain poses and become a global mobile payment service (Vilmos & Karnouskos, 2003). We present in the rest of the chapter a detailed description of the approach, its implementation, and features that diversify it from other systems and make its future promising.

MOBILE PAYMENT SOLUTIONS

A mobile payment solution can be used in multiple applications and scenarios. The simplest scenario involves only the user, the device and a single payment processor, such as a mobile operator, bank, broker or an insurance company. The user identifies himself to the mobile device through secure identification mechanisms, including physical possession and password or even via biometric methods; the device then authorises the transaction to the payment processor for money transfer. More complex transactions involve at least one additional party, the merchant. In this case, the merchant may be affiliated with a different payment processor; therefore the two payment processors must be able to interoperate.

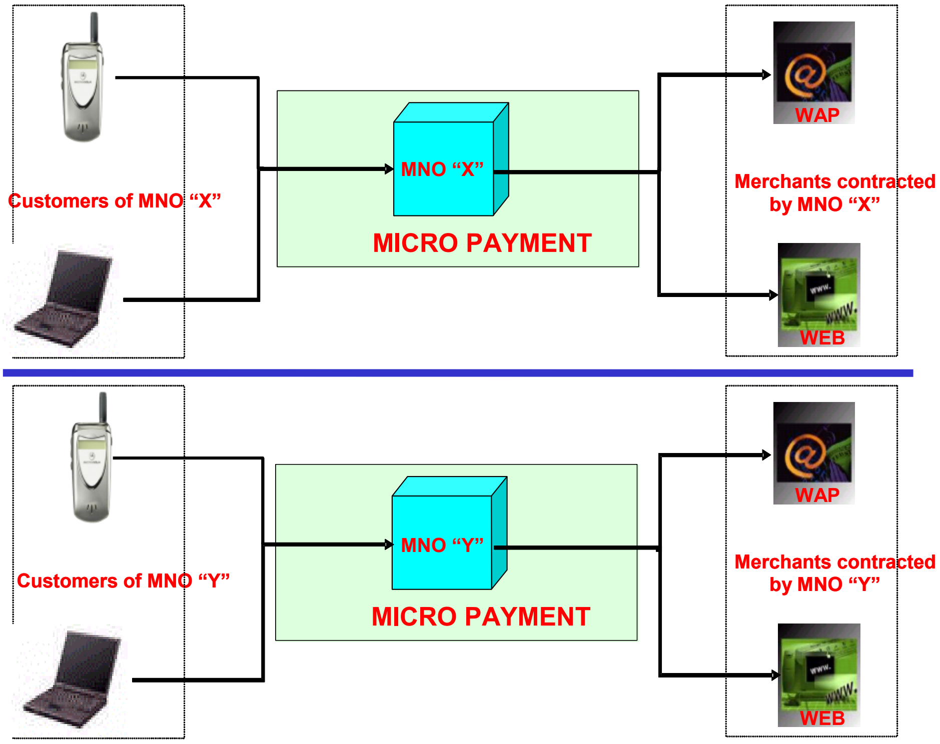

Figure 1 –Existing m-payment solutions

Most of the existing mobile payment solutions such as NewGenPay (www.newgenpay.com) and m-pay (www.m-pay.com), assume that a mobile payment service is offered to the customers of a particular mobile network operator, MNO, as shown in Figure 1. These payment solutions allow customers of a particular mobile operator to perform payment transactions with merchants who are contracted by the same mobile operator, (the payment processor, in this instance). In these payment solutions, no cross-over to other operators is foreseen, no direct involvement of trusted organisations, such as banks, takes place and, hence, payment transactions are limited to micro-payment transactions only, typically under 2 €. Although existing payment solutions have provided the critical mass for the adoption of mobile commerce, they offer limited transaction potential and limited accelerator effect of mobile commerce (Henkel, 2001).

In this chapter we present a secure mobile payment service (SEMOPS, 2003), a mobile payment solution that is capable of supporting micro, mini (e.g., between 2 € and 20 €), as well as macro payment (e.g., over 20 €) transactions. It is a universal solution, being able to function in any channel, including mobile, Internet and POS; it can support any transaction type, including P2P, B2C, B2B and P2M (person to machine), with a domestic and/or international geographic coverage. As shown in Figure 2, SEMOPS enables the realisation of a mobile payment network that combines different payment processors, and, hence, it can realise a payment service with huge transaction potential, lower user fees and large turnover (Kreyer et al., 2002).

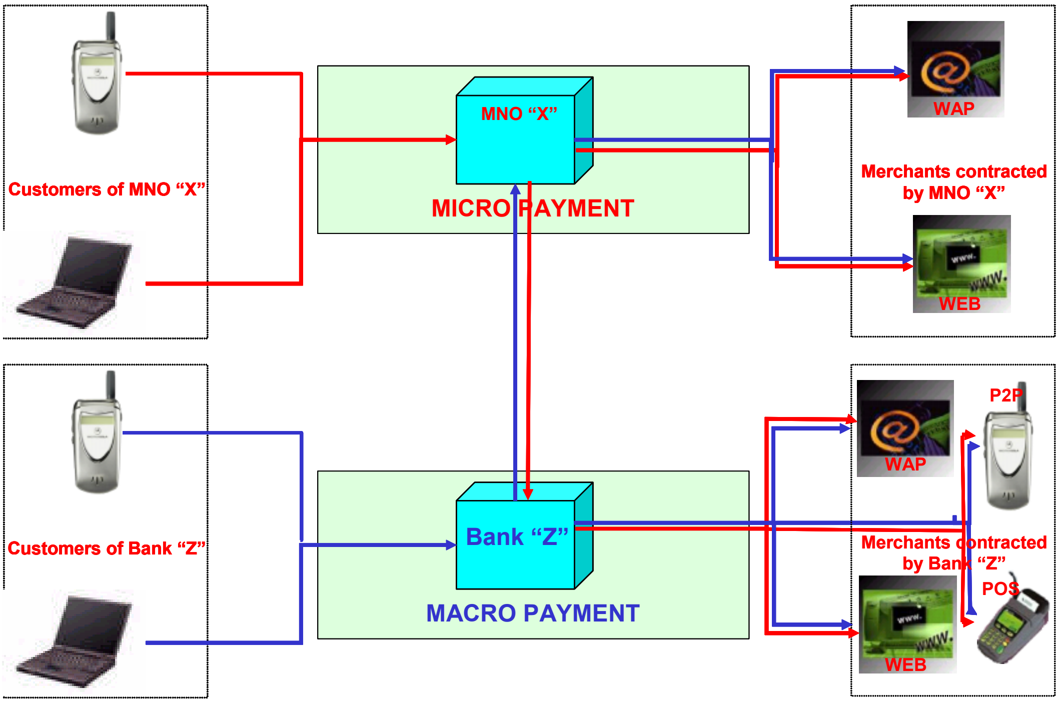

Figure 2– SEMOPS m-payment solution

As shown in Figure 2, the SEMOPS payment solution allows both, mobile operators and banks to become payment processors in a mobile payment service. There can be different combinations, depending on whether the user uses his bank or MNO account and whether the merchant accepts the payment on his bank or MNO account. Furthermore, the SEMOPS model is versatile and any trusted service provider that can offer the customer an account (e.g. credit card, financial service provider) can also easily take the role of the SEMOPS payment processor.

SEMOPS TRANSACTION ARCHITECTURE AND FLOW

As in every payment system, SEMOPS is capable of transferring funds from the customer to the merchant, or, in more general terms, from the payer to the payee. Typically, this transfer is realised via a payment processor, such as a bank or a mobile operator. The SEMOPS payment solution, however, is novel in that it enables cooperation between different payment processors, e.g., cooperation between banks and mobile operators, in achieving a global, secure, real time, user-friendly and profitable mobile payment service that can be used in both electronic and mobile commerce transactions.

SEMOPS supports both, remote and proximity transactions. In remote transactions, which are conducted independent of the user location such as prepaid top-up services, delivery of digital services, mTickets, digital cash, peer-to-peer payments etc., payments may be conducted via several communication channels that include SMS, USSD, WAP push and Instant Messaging, and manual input. In case of proximity transactions, however, where both payer and payee are at the same physical location, the payer's mobile device may communicate directly, (e.g., via Bluetooth, IrDA, RF, NFC) with a POS/ATM such as payments at unattended machines, mParking, payments at traditional POS, or money withdrawal from a bank's ATM. If the technical capabilities of the involved devices do not cater for direct communication, the communication channels supported for remote payments can be used, instead. Note that, the payers can authorise payments by both mobile devices and web browsers, whereas payees can participate with any sale outlet, including WAP, POS, vending machines, or web. Moreover, SEMOPS can support mobile Person-to-Person (P2P) transactions with the same convenience as any other payment transaction.

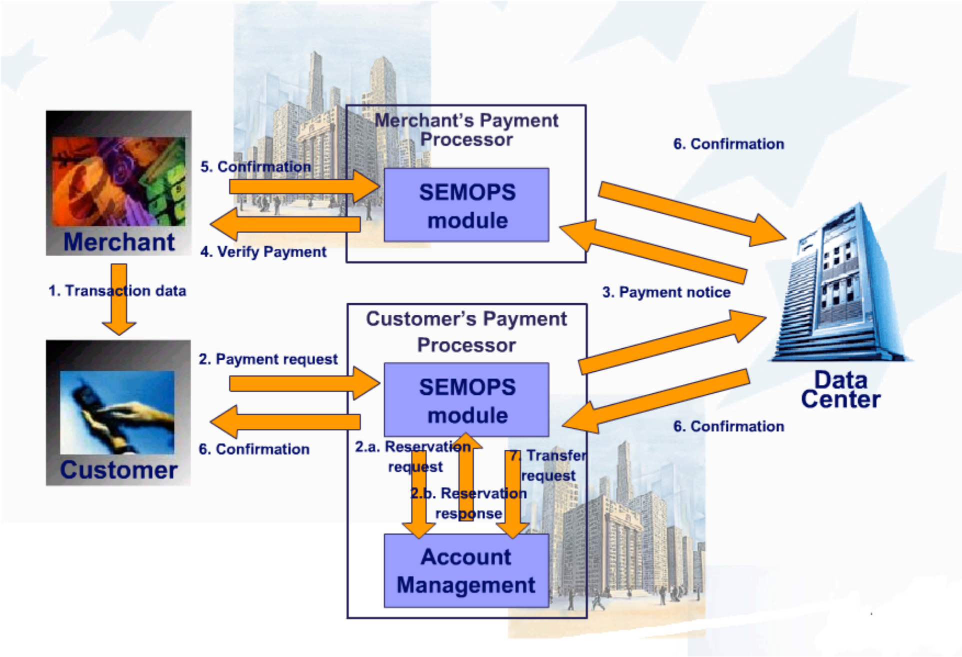

Figure 3 – SEMOPS Transaction Architecture

In SEMOPS, payment requests are completed in real time. However, in case where the payee is not connected to its payment processor, the payment is still going to be credited and the payee will be notified at some later time (offline payments).

The transaction flow, which is completely controlled by the payer, follows a simple credit push model. A typical SEMOPS transaction flow for a prompt payment from a customer to a merchant is discussed in the following, (see figure 3):

- The merchant (in general, any POS/VirtualPOS) provides to the customer the necessary transaction details (e.g. via IrDA, Bluetooth or even Instant Messaging), (Step 1). This data includes certain static and dynamic elements that identify the merchant and the individual transaction. During the whole payment process, the customer does not identify herself to the merchant, nor does she provide any information about herself, her bank, or any other sensitive data.
- The customer receives the transaction data from the merchant. (Step 2). A standard format payment request is prepared to be sent to the selected payment processor who is the trusted partner of the customer – either her bank or her mobile network operator. When the payment request is ready for transfer, the customer checks its content, authorises it (via PIN and/or PKI), and sends the payment request to the selected payment processor.

- The customer’s payment processor receives the payment request, identifies the customer and processes the payment request, (Step 3). Processing includes the verification of the availability of the necessary funds, and reservation of the required amount. When the processing is completed a payment notice is prepared by the payment processor and is forwarded to the Data Center of the SEMOPS service. The Data Center identifies the addressee bank of the payment notice and forwards the message to the merchant’s trusted payment processor, who again can be either its bank or mobile operator. The Data Center handles the message delivery among the payment processors. We assume that at least one Data Center per country will exist, and in case of an international transaction a second Data Center is also involved, namely the local Data Center of the foreign merchant’s country. The two Data Centers cooperate and the transaction is routed accordingly.
- The merchant’s payment processor receives the payment notice and identifies the merchant. The payment processor advises the merchant in real time about the payment by forwarding the payment notice (Step 4). The merchant has the chance to control the content of the payment notice and can decide, whether to approve or reject the transaction. By confirming the transaction to its payment processor, (Step 5), a confirmation through the Data Center to customer’s payment processor is forwarded (Step 6).
- When customer’s payment processor receives the positive confirmation, it initiates a regular bank transfer to merchant’s bank. This transfer is based on the regular well-established inter-banking procedures. In case of successful money transfer, the merchant’s bank sends a notification to the merchant, and the customer’s payment processor sends a notification to the customer. If for whatever reason the merchant rejects the transaction, the customer’s payment processor releases the funds it has reserved for the purchase.

SEMOPS FRONT-END INFRASTRUCTURE

Unlike the PC environment, the mobile environment presents the challenge of supporting multiple data channels and platforms. Mobile communications are characterised by the variety of data technologies, device capabilities, and standards. Shopping and payment may take place on separate channels. For example, a customer may shop via WAP or receive an actionable alert, and carry out the payment over SMS, USSD, raw GPRS or WAP to the payment processor. Therefore, in defining mobile solutions, it is important to recognise that multiple technologies coexist, and will continue to do so.

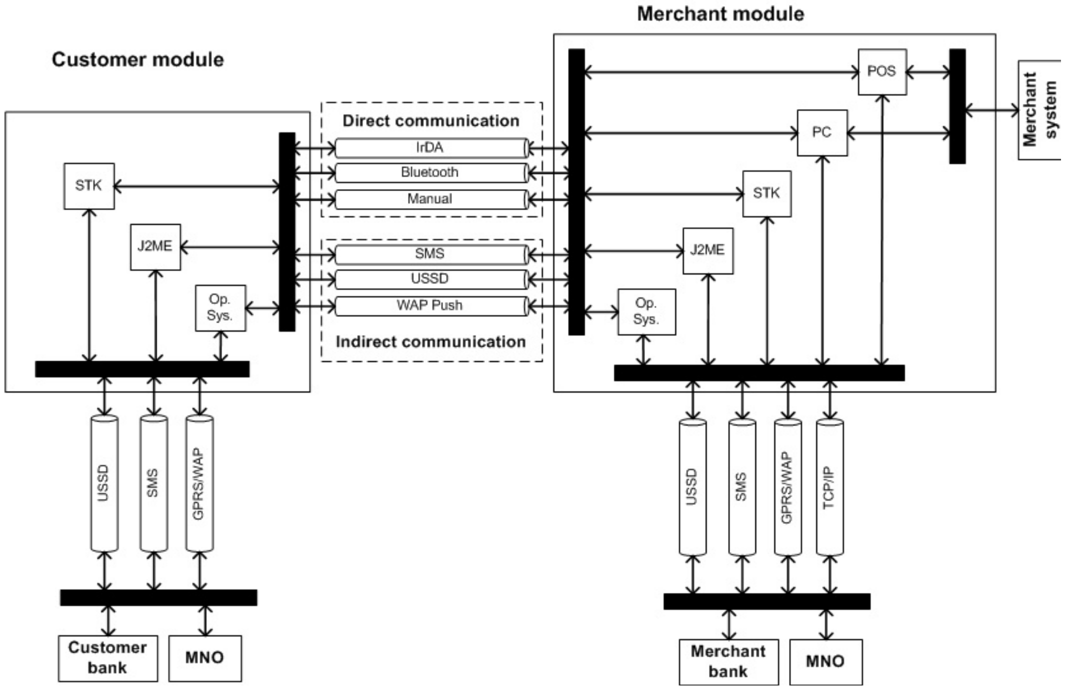

Figure 4 - Base Technologies of Front-End Modules

As a result, the SEMOPS infrastructure became very colourful from mobile technology point of view and combines all viable implementation possibilities. It utilizes SIM Toolkit (STK), Java phones (J2ME) and embedded operating systems (OS) as the application executing environment and various transmission technologies:

SIM Application Toolkit: The SIM Application Toolkit (SIMToolkit or STK) defines the necessary set of commands and procedures required building the basic SIM Card – Mobile Equipment interface for mobile equipment independent applications running on the SIM card. The standard has broadened from data download and the proactive SIM approach to a powerful tool-set for several types of applications enabling network operators to develop competitive and differentiated applications.

Java 2 Micro Edition: The Java 2 Micro Edition (J2ME) is a popular standard among major handset manufacturers. Most handset manufacturers have already launched at least one pilot mobile with J2ME capability. The mobile phones are mainly supporting the MIDP 1.0 (JSR-037) and the CLDC 1.0 (JSR-030) Java recommendation. MIDP supports the Java Sandbox Model very much like the applets that run in web browsers. In this context each MIDlet runs in its own environment and cannot affect other MIDlets. MIDP 1.0 is capable to start HTTP connection to a server. The nature of the http connection is that the MIDP client sends GET and POST commends to get info from the server application. This means server push is not available in MIDP 1.0 (only with some tricky workarounds). MIDP 2.0 implements server push.

Embedded Operating System: Most of the popular mobile phones and smartphones are using proprietary OSs today. SEMOPS focuses also on the commonly used mobile phone and PDA OSs that support Java. To our opinion only a small set of the high-end mobile phones and smartphones, will use rich-feature java-enabled OSs in the next years, but in the long-term this percentage is expected to increase.

THE CUSTOMER AND MERCHANT MODULES

The main modules in the SEMOPS solution are the front-end modules, namely, the customer and the merchant modules. These are designed to have extended functionality, security, openness, usability and a versatile application-executing environment. The back-end modules comprise of transaction management applications that reside in the payment processors' premises and interact with their accounting systems, as well as the Data Centre modules, which is responsible for the communication and reconciliation of transactions between involved payment processors. As shown in Figure 4, the SEMOPS front-end modules are very versatile from the mobile technology point of view and combine all viable implementation possibilities in user-process and client technologies.

The customer module: It has two basic forms, the mobile and the Internet one. A variety of implementations exists in the mobile form, namely, a SIM toolkit (STK) based, a Java based and an operating system (OS) based module. The customer module assists the customer to carry out a payment transaction using the service. The module can be downloaded and updated over the air or from the Internet, thus, avoiding the usual hassle one has to go through, when subscribing for a service. The actual payment functions include communication with the merchant's systems, preparation of payment request, communication with the selected payment processor, administration of the transaction details, and notification of the user about a transaction status.

The Merchant Module: It is the bridge between the payee's sales outlet and the payer, and also between the payee and the payee's payment processor. For this reason, the merchant modules include an Internet and a POS version, along with multiple mobile versions (STK, Java, OS). The merchant module receives the necessary transaction information from the merchant's sale system and transfers it to the customer. An important function of the merchant module is the approval of the transaction. The merchant's payment processor advises the merchant about the payment and the module either approves or rejects the transaction automatically based on the information it has. The merchant module features also extensive administrative functions e.g. report generation refund initiation etc.

SECURITY CONSIDERATIONS

SEMOPS built up its security framework at the payment processors with the following considerations:

- Banks do not allow encrypted information into the Intranet; therefore decryption must be done in the Demilitarised Zone (DMZ).
- Banks usually have their own authentication system, therefore SEMOPS must co-operate with existing infrastructures.
- SEMOPS uses heterogeneous channels, including more rare ones, like USSD, therefore SSL cannot be always used as encrypted channel.
- Different country regulations prohibit the usage of the same keys for encryption and signing; therefore SEMOPS must have multiple key pairs.

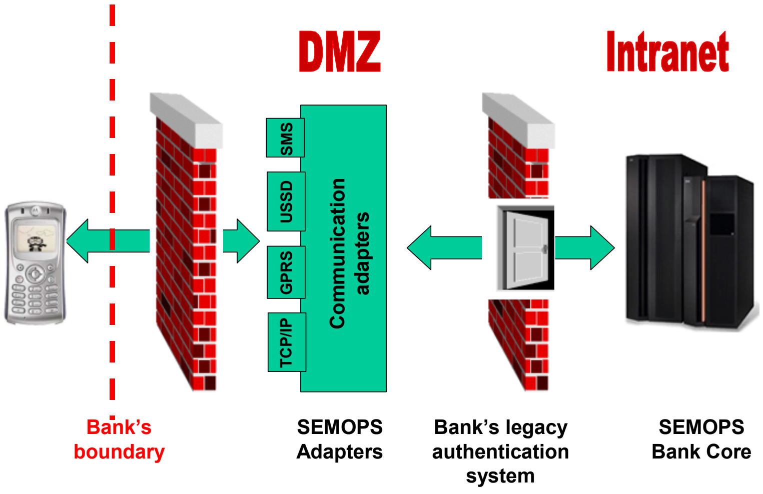

Figure 5 - Security infrastructure at payment processors

Based on these limitation SEMOPS utilizes the security approach depicted in Figure 5. The termination of the physical channels and the decryption of the messages is done in the DMZ. The decrypted information reaches the SEMOPS Bank Module (residing on the Intranet of the bank) through the bank's standard authentication system, which is already used for applications, like home banking. Currently SEMOPS uses RSA encrypted XML with 3DES message keys, and also uses RSA digital signatures on the messages, but with a different key pair. The hardware security modules execute all the cryptographic operations in the system, resulting in the split security operations depicted in Figure 6.

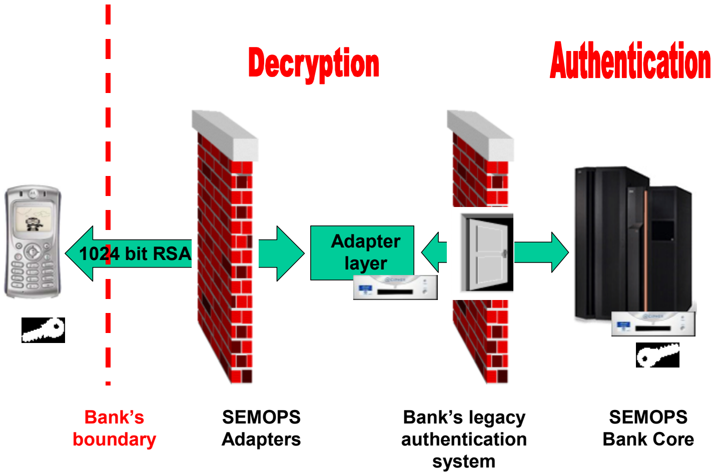

Figure 6 - Split security operations of SEMOPS

SEMOPS uses dual authentication method for identity control. Depending on the payment processor's requirement it is able to use digital signatures or encrypted pass-phrase authentication. The payment processor can decide, which authentication method to use, although digital signatures require a trusted third party to vouch for the authenticity of the public key used to verify the signature. At that point the recipient is sure that:

- The original data was not altered (data integrity);
- The message could only have been signed by the holder of that private key (entity authentication); and
- A trusted third party(TTP) has vouched for the fact that the signer is in fact the holder of that key pair.

Therefore, the uniqueness of the digital signature and the underlying hash value coupled with the strength of the public key certificate provides an acceptable level of assurance to authenticate the sender and to verify that the sender was the originator of the signed data.

With the basic considerations above, SEMOPS provides a strong end-to-end encryption for transferred data and allows the usage of different authentication techniques embedded into this encryption. This seems a viable solution, but in live environments it must be adapted to the usual practices of banks, which insist on not allowing anybody else to authenticate their users, as this task has to remain within the banks' legacy procedures.

APPLICATIONS AND BUSINESS SCENARIOS

The SEMOPS solution is a universal solution that allows payment for goods and services in, practically, any kind of commercial situations. As shown in Figure 7, SEMOPS is a global payment service that can be a viable cash substitute for various types of e/m-commerce transactions. The *Customer* (payer) and the *Merchant* (payee) exchange transaction data and then the fund transfer is performed by the corresponding trusted payment processor, i.e., the *Customer's* and *Merchant's Banks*, respectively. The Data Center simply routes the information flow between the actors and is responsible for the reconciliation of the transactions.

To understand the basic philosophy behind the operation one has to see, that all transactions, irrespective of the channel, value, commercial situation and terms, are using the very same infrastructure, the same solutions and processes, and are settled and protected by one service. This uniformity allows unparalleled efficiency. The specifics of the revenue and cost side result in favourable commercial terms for the users and in high-level profitability for the operating actors.

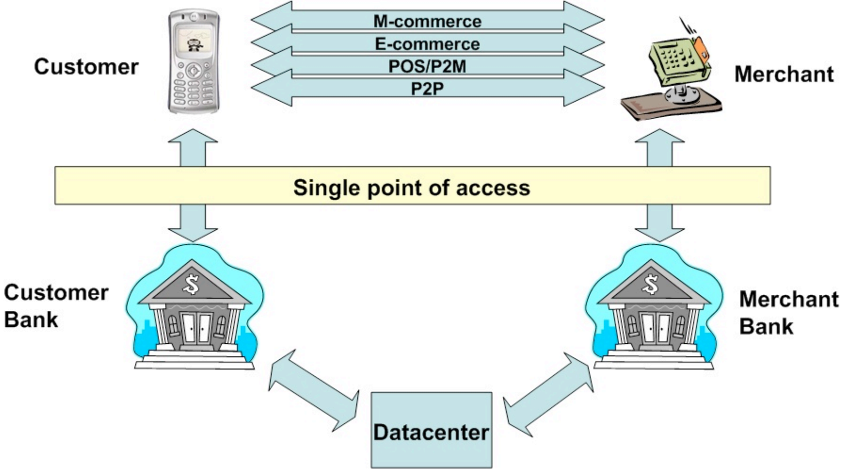

Figure 7 - Overview of SEMOPS (Bank-based model)

In the following, we examine how SEMOPS operates in certain situations:

- Purchase of mobile content
- In-band transaction

- POS payment: P2M
- P2P payment
- EBPP and
- Internet payment: B2C, B2B, Auction.

PURCHASE OF MOBILE CONTENT

Digital content will have one of the largest shares of revenue generated in mobile commerce. Important elements of this category may be, ring tones, logos, games, music and videos, information, on-line gambling, and adult content. A customer browses the web using her mobile handset and wishes to buy digital content. The customer selects the product, and pushes the payment button on the site. Having initiated the payment, the customer receives the payment information onto the handset she has used for the browsing.

Knowing that the value of digital content is quite low, the customers have the option to pay from their bank account or from the prepaid/post-paid account with their mobile operator. Having decided which account to use, the customer selects her payment processor of choice from a menu in the handset (there is always one default payment processor to accelerate the transaction flow) and prepare the payment request. After validating the transaction e.g. with a PIN, the payment request is sent to the payment processor. If the transaction is approved by the merchant, then in a matter of seconds a confirmation is received by the customer that also includes a link where the content can be accessed.

IN-BAND PURCHASES

The process of making in-band payment transactions is quite similar from a technical point of view to the above digital content scenario, the key difference being the value and delivery of the goods and services. In-band purchases also include widely varying products and services and the special features of these needs to be taken into account. Key applications may be parking payments, various kinds of ticket purchases and payments made to online stores through a mobile device. Purchase can be made through browsing, locating the product and selecting payment as in the case of buying digital content.

In case of payments for parking, a more convenient solution is preferred as this will usually be a repeated transaction. The customer can store details of the parking company in a template, and also the license plate of his/her car. By just sending the payment request to the payment processor the parking company is advised of the payment, and grants a parking permit for the time that the customer paid. In the confirmation received from the payment processor, the customer is also advised about time period he has paid for. When the controller finds a car without a valid ticket, he first communicates with the central database and he may be advised that the specific car has paid for parking through a mobile device. An additional advantage of this solution is that, should the driver need to stay longer than originally expected, he can extend the validity of the permit even from a remote location, without the need to go to the car or to the parking meter.

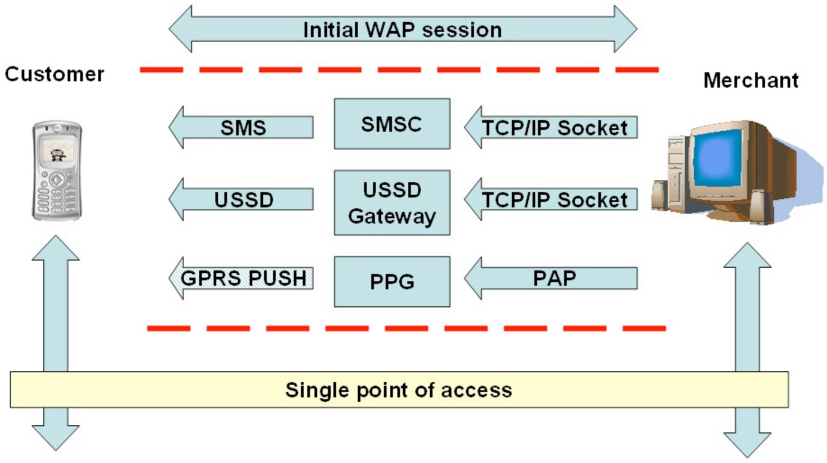

Figure 8 - In-band purchases in SEMOPS

The top up of mobile pre-paid accounts could also be considered as one type of in-band transaction. In this case the customer is practically buying airtime from the mobile operator by putting money onto the prepaid account. The customer prepares a payment request and requests from its bank, its payment processor, to send money to the MNO, the merchant, in this case. As soon as the payment information arrives to the MNO, the top up can take place and calls can be placed again. If the MNO had a service to actively inform the customers that their pre-paid balance was running low, the mobile payment could ensure continuous availability of the pre-paid phone service.

P2P PAYMENT

Today, there is no real widely adopted solution for mobile Person-to-Person payments in the same currency, not to mention international transactions. Using the SEMOPS solution, payment can be made to anyone having a mobile handset in a matter of seconds and the money sent can also be available for use immediately.

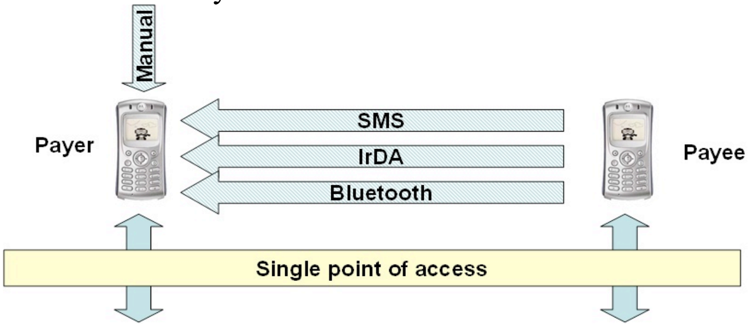

Figure 9 - P2P payment in SEMOPS

There are three basic scenarios in P2P payments:

- If the two parties are in the proximity of each other, the payee's device sends the transaction data over to the payer's handset using either IrDA or Bluetooth communication.
- If the two parties are not in the position of using direct link, the payee can send the necessary info over the air (e.g. SMS or instant messaging) to the other person.
- In certain cases, the payer initiates a transfer while the payee may not even be aware of the fact that he is going to receive money. In this case, the payer can

manually input all necessary information into the handset and can start the payment process without advising the payee in advance.

Depending on the transaction value, the payer in all three cases has the option to select either one of its banks or his MNO for processing the payment. The payment processor performs the payment and the beneficiary's payment processor confirms the transaction if the payee really exists. The payee will also receive the payment notice on his mobile handset in real time, or will be notified when he turns his mobile on, if he was offline at that moment.

Point of Sale (POS) payments

POS payments are well known for purchases made in stores where credit cards are accepted. The mobile POS version supported by the SEMOPS service is slightly different from the traditional solution. This difference, however, makes the payment considerably more secure and trusted. In the case of a SEMOPS POS transaction, the POS terminal has to be modified. Today the new EMV conformant terminals can be easily extended and have also a number of SAM card slots to allow simple programming and modifications. After having made this typically minor modification, an IrDA device is plugged into the serial port of the POS, and the POS is ready to perform mobile payments.

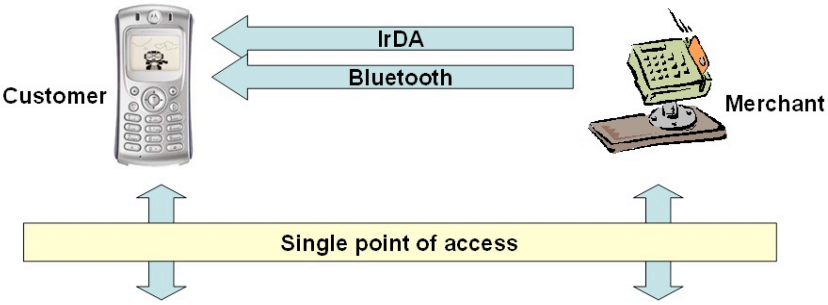

Figure 10 – POS/P2M payment in SEMOPS

In a typical scenario, after shopping in a store, the customer goes to the cashier to pay. When the cashier finishes entering the purchased items into the merchants system, a standard non-cash transaction is initiated. The POS receives the transaction data from the cashier either automatically or manually. At this point the customer may decide to pay using the mobile payment service. The mobile handset receives the transaction data from the POS terminal through the IrDA communication (alternatively, an SMS can also be sent to the customer's mobile if it does not have an IrDA port). Having received the necessary information, the mobile device prepares a payment request that is validated by the customer (PIN) and it is sent to the payment processor. Depending on the purchase value, the customer may decide to send this information for processing, either to her MNO or to her bank. The cashier receives the payment authorisation in the POS terminal just like in the case of traditional card transactions.

P2M (vending machine):

Buying from a vending machine and paying it electronically, is equivalent to making a payment to an unmanned POS terminal. The only difference is the way the transaction data is forwarded to the POS terminal. In the case of a vending machine, the customer selects the product and by initiating the transaction on the vending machine the transaction data is forwarded to the handset. When the payment is performed, the vending machine receives the authorisation and provides the selected product. A similar approach is provided today by calling a premium number, however this is product specific and not as flexible as the SEMOPS-enabled payment. The unmanned POS scenario is one that may have huge potential in future stores. Should the customer wish to avoid queuing at the cashier, she can have the purchased products valued automatically by a scanner and can make the payment without the need to communicate with the clerk at the cash register.

ATM

Even if it is assumed that a universal mobile payment solution will be used in all types of transactions, need for cash payments will still exist. Withdrawing cash from an ATM is very similar to buying a coke from a vending machine; the only difference is the type of sold product. An ATM sells cash while a vending machine sells tangible goods. The SEMOPS solution can be easily used in realising ATM withdrawals in a global base, meaning that any service user in any country at any bank can get the desired cash.

EBPP (MBPP)

Electronic Bill Presentment and Payment (EBPP) transactions with SEMOPS are placed between mobile and Internet payments. The summary of an invoice can be sent to the mobile device, whereby, if the structure of the information matches the SEMOPS required format, the customer can also pay the invoice with the regular procedure. Would however the customer be interested in the invoice details, he can visit a dedicated site on the Internet and perform payment on-line.

INTERNET PAYMENTS

B2B, B2C: Payments with the SEMOPS solution can also be realised on the Internet. While browsing the web, the customer finds the desired product. After placing it into the shopping cart, the customer selects the SEMOPS payment option. The merchant e-shop provides the transaction data to the customer over the web. The customer receives the data, and using a dedicated software application prepares a payment request on her screen. The customer authorises the payment, e.g. with her PIN, and sends the payment request to her bank. During the whole procedure the customer did not provide any sensitive data to the unknown Internet merchant. Through the usual SEMOPS procedure, the payment request is processed by the customer's bank.

Auction payment: A unique transaction type with increasing importance is the purchase at auction sites. The peculiarity of this type of transaction is that the customer wishes to see the product first before payment is performed, but the merchant also wants to make sure that he will receive the purchase price. The solution is the escrow service provided by the auction house to be supported by the SEMOPS payment service. In this case, a payment request contains information both about the seller and the escrow agent. The payment is processed at the customer's payment processor and the merchant receives only a conditional payment notice. The merchant will only be paid if there is no customer complaint within a limited period of time. The money in the meantime is sent to the auction house, which plays the role of the escrow agent. If there is no customer complaint, the money is forwarded automatically – without the involvement of the escrow agent – from the escrow agent's bank to the merchant's payment processor. If, however, the customer complains, payment is stopped until the escrow agent investigates the issue, and, based on its findings, the money is either refunded or paid out to the merchant.

SEMOPS BUSINESS MODEL

As with any other new payment solution, SEMOPS should make good economic sense for its key players. All the advantages offered to the end users, i.e., the security, the convenience, and the wide reach of transactions, may be in vain if there are no economic incentives for the key actors (Camponovo & Pigneur, 2002). It is also obvious that the operating actors alone cannot make a success story of the payment solution, if the users are dissatisfied either with the service, or with the usage terms (Heijden, 2002).

ACTORS AND THEIR INVOLVEMENT AND INTERESTS

The key actors in the SEMOPS model include, as shown in Figure 11:

- **Operating actors:** International Operator (IO), Local License Holder (LLH), Data Center (DC), Risk Managers (RM) and the Local Payment Processor (LPP), which as noted before can be different entities e.g. a bank, a mobile network operator (MNO) or any other service provider (OSP).
- **User actors:** Customer and the Merchant (any type of real/virtual POS)
- **Additional actors:** Developers, auditors, service providers, suppliers, etc.

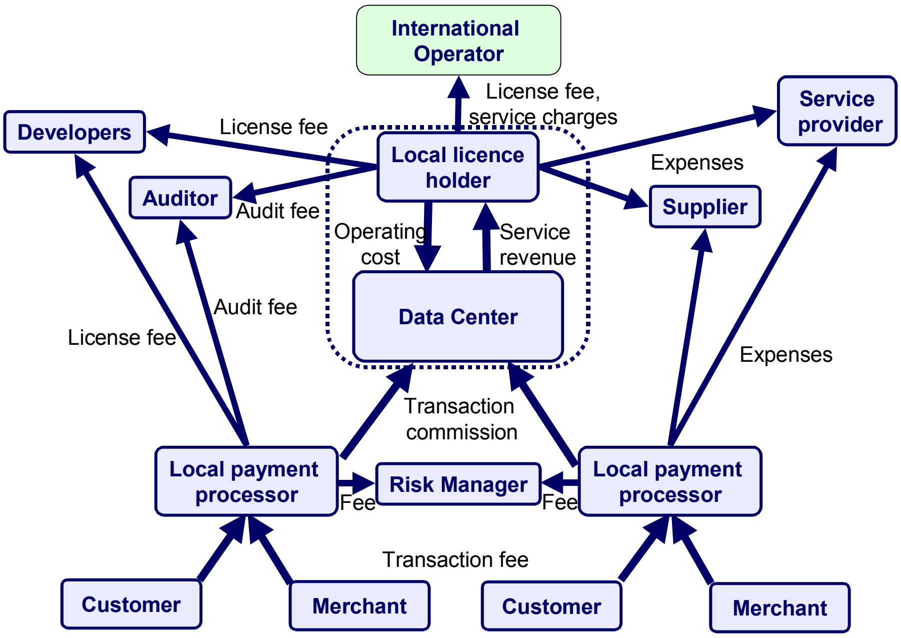

Figure 11 - Business relations of the SEMOPS actors

The *International Operator* (IO) is the entity responsible for the coordination and development of the service on international level. The *Local License Holder* (LLH) is the entity that is in charge of the local operation of the SEMOPS payment service that owns all the rights in relation to this service. The local *Data Center* (DC) operates the Data Center module of the payment service. The *Risk Manager* is charging a fee to the Local Payment Processors for the services it provides. *Local Payment Processors* (LPP) are entities that provide the SEMOPS service to the users. The *Customers* and *Merchants* are clients of LPPs. The *Developers* are the software development teams, providing the software modules that form the basis of the SEMOPS payment solution or its extensions.

Finally, the payment service is a complex operation that needs external services and products from a number of *service providers* and vendors, who have no affiliations with the payment service itself.

BUSINESS CONCEPT

Primary principle of the business model of SEMOPS is that it is based on the cooperation of banks and MNOs. This situation has two consequences:

- resources can be combined, and
- net revenue has to be shared.

The business concept of SEMOPS was formed by taking into account the following considerations.

- Firstly, the banks involved in the new service have already electronic payment services, and while SEMOPS may offer increased market presence and new transaction channels, it has to be more profitable than existing services.
- The MNOs are already involved in a number of payment initiatives, or are completely disinterested in this line of business. One of the key challenges of the SEMOPS solution is to integrate micro payment services with mini and macro payments, which are typically performed via banks, into a combined payment service, a business prospect, which MNOs find attractive.
- The SEMOPS service should offer increased potential for the mobile operators in terms of customer reach, product scope, and most importantly in terms of value added new revenue channels.
- Customers have the full spectrum of services and products to buy with the new payment service in a number of purchase situations and via different communication channels. This benefits the customers, but the level of this benefit differs according to each transaction type. Consequently, in certain cases purchase fees are not acceptable.
- Finally, the associated expenses keep the majority of merchants away from mobile payment schemes. Consequently, SEMOPS overall transaction costs, (including set up expenses), have to be below existing levels of electronic payments, and the approach has to address as many payment procedures as possible (Kreyer et al., 2002) in order to reach the critical mass.

SEMOPS IMPLEMENTATION EXPENSES

SEMOPS has a relatively low implementation costs due to several factors.

- Firstly, the solution is fully automated and there is end-to-end electronic processing. As a result variable expenses are minimal and introductory expenses can also be well controlled through a modular and scalable implementation approach.
- The standardisation of the service processes, and technology will further reduce both introductory and operating expenses.
- Installation of the new service modules is based on middleware technology, and by offering the service on a number of different operating platforms the introduction will be simple and cost efficient.

- The operation of the SEMOPS service also has a number of factors that allows optimisation of resources. The payment processing is allocated to those organisations that can perform this activity within their existing operating framework with marginal extra expenses, such as banks. To allocate micro payment to mobile operators and larger values to banks provides an operating optimum.
- Similar is the case with the Data Centers, whose operation, at least at the launch of the SEMOPS local services, will be performed by existing service providers. Much of the cost of operation could be incurred through communication, the settlement process and through security related solution.
- The secure process flow, the applied hardware and software solutions, the homogenous rules, regulations and processes, and the continuous audit activity will minimize the security risk and as a result reduce related expenses.

SEMOPS Revenue Generation

The potential revenue generation in SEMOPS service is based on the following considerations:

- SEMOPS customers base combines the customer base of participating banks and mobile operators.
- SEMOPS combines different transaction channels, i.e., mobile (in-band), internet, traditional (POS, P2M).
- SEMOPS combines different transaction types i.e. C2B, B2B, and P2P.
- SEMOPS combines different payment values i.e. micro, mini and macro payments.
- SEMOPS offers large geographical coverage, i.e., domestic and cross border.

Figure 12 depicts the major revenue streams for the key operating actors, i.e., the mobile operators and the banks. It contains only the service related revenue sources and does not include revenue streams for the associated parties. Those revenues will have to be derived from these channels. Figure 12 also contain those potential revenue streams that are uniquely associated with SEMOPS. For this reason, the normal communication revenues that are associated with the use of the telecommunication infrastructure in any mobile communication activity are not shown.

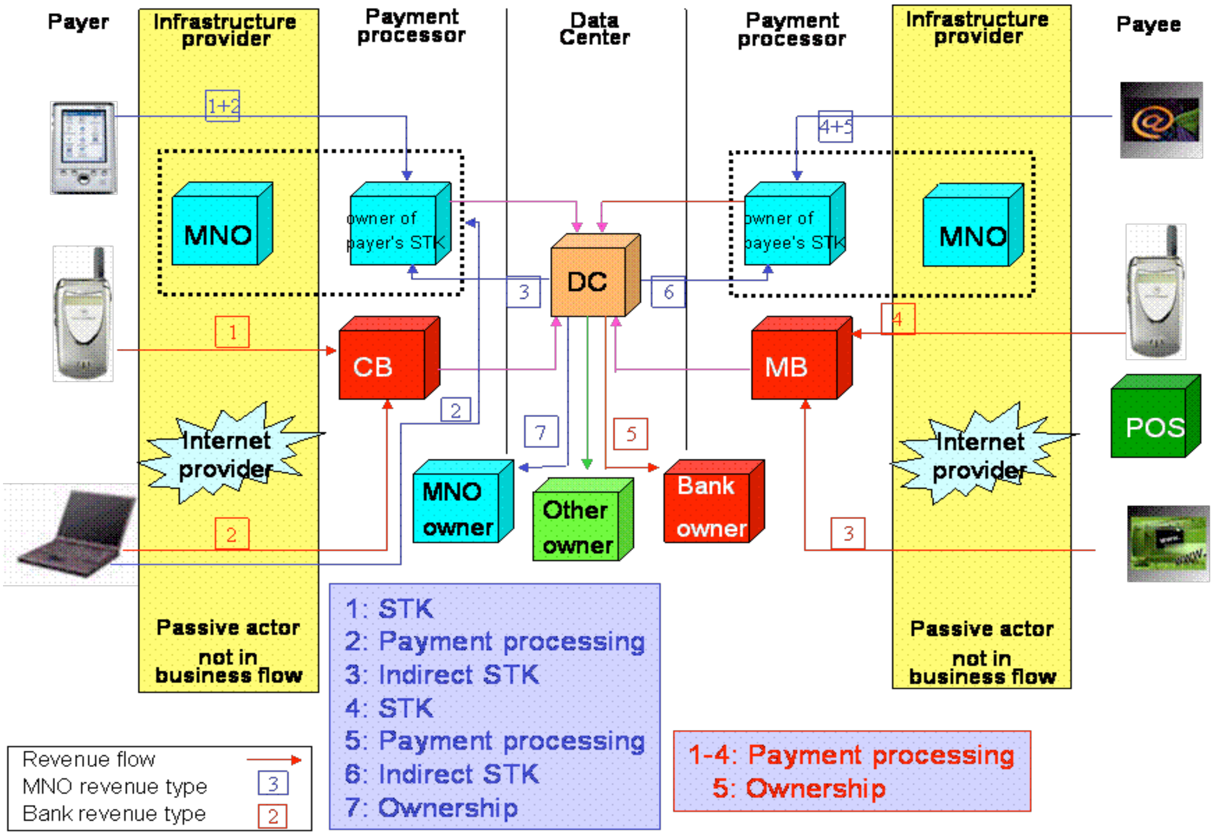

Figure 12 - SEMOPS Revenue Streams

Let us note, once more, that a third party service provider, (e.g. credit card companies), can easily slip into the role of banks in the SEMOPS model, and, therefore, benefit from the revenue streams mentioned above.

EVALUATION OF THE SEMOPS APPROACH

SEMOPS was designed and developed so that it can operate in commercial electronic channel on Internet and mobile infrastructure. The key features of the SEMOPS payment solution, which constitute the main differences from existing payment services, include:

Security, Trust and Privacy: With existing electronic payment services, the customer provides her personal information to a merchant or to other third party service providers without controlling the subsequent use of this information. It is of no surprise that many people avoid making electronic payments due to the imposed lack of privacy. In SEMOPS, the customer communicates only with her trusted partners, i.e., her own Bank or Mobile Network Operator, and she does not provide private information either to the merchant or to any third party operator. This prevents possible misuse of the customer's sensitive information, and the transaction cannot be repeated by anyone else, at any other time. Furthermore, SEMOPS allows the customer to retain his anonymity against the merchant, if he wishes so. In this way, anonymous payments are possible, which can be a real substitute for cash. Moreover, due to the credit push concept adopted in SEMOPS, the customer is the driver of the payment process. Nothing can happen that the customer would not approve or agree with. The customer personally approves all transactions and sensitive personal information is not stored in the system. Transaction details are only captured at one's own payment processor.

Furthermore, the money received or spent via the SEMOPS solution are moved always from the user's account, therefore there is no need to "preload" any money to use the service, nor the money gets lost if the user looses his device, as in e/m-Wallets approaches. Trust and security is ensured on the merchant's side, as well. Although the merchant may not know, who the actual buyer is, his trusted payment processor guarantees the payment to him. The merchant really does not care whom the money is coming from, but he needs a guarantee that he will be paid for a certain transaction. The SEMOPS service ensures this in real time, and as such, increases the trust in the system. Finally, SEMOPS has several security services in place in order to make the service as secure as possible, from the technology point of view. SEMOPS provides a strong end-to-end encryption for transferred data and allows the usage of efficient authentication techniques embedded into this encryption. SEMOPS also takes advantage of the "social security feeling" and existing long year trust relationships between customer/merchant and their respective payment processors, e.g., bank or MNO. There is a feeling of trust in the SEMOPS system that it can substantially contribute in the rapid expansion of the service.

Speed: There are many services around which consider themselves electronic payment solutions, however, the speed they perform the transactions, not to mention the settlement of the transactions, is slow and inadequate even for traditional purposes. SEMOPS is different from this point of view, as the approval of the transaction is performed within seconds and in certain circumstances even the actual money is available for use immediately for the beneficiary. This speed allows the introduction of such new transaction types like P2P payments, where the beneficiary can spend the money received right away.

User friendliness: Existing e-payment solutions are either cumbersome, slow, or are specifically tailored for a limited clientele, on the customer or merchant side. If someone needs to type all his payment details, and if this typing needs to happen on a handset with 12 keys, chances are that the person will think twice whether to perform the transaction. SEMOPS is very much user centered. All user specific information can be stored locally either on one's handset or in the PC and the information stored is not sensitive. Payment is performed from a special menu that is identical both on the mobile handsets and on the PC, to ensure a homogeneous user experience. The latter is further enhanced through the fact that all different payment types supported by SEMOPS follow the same pattern and same procedure, to increase the comfort of the customers. As menus are assisting the users, the actual typing is reduced to a minimum, namely, to menu selection and the input of a PIN.

As mentioned before, transactions can roam many devices, therefore it is possible to initiate the transaction on one device and continue it on a different one, e.g., enter the transactions on one's PC and then simply activate them via one's mobile (after synchronizing with the bank). To assist conflict solving between customers and merchants a special refund function is also part of the SEMOPS service, built into the same menu that is used for payment purposes.

In a broader sense, user friendliness also includes such aspects as ease of registration to the service, access to the service, scope of use of the service, internationalism etc. Although registration policy depends on the individual payment processors, theoretically electronic registration is possible, and one can start to use the service without the need to visit any branch office, or meet any customer service agent. The service is offered to the public primarily by banks and mobile operators. This concept means that not only a handful of selected ones could enjoy the benefits of SEMOPS, but it can be made available online to a wide group of people – something very interesting for people living in rural areas. This potential wide reach also ensures that a large number of merchants can be paid through this service, and also merchants can serve a large clientele. This scope is even further increased by the fact that the service is designed for international operation allowing cross border, international transactions to be made.

Cooperative approach: Most existing electronic payment services are offered by a single entity or a closed group of entities to a limited clientele. The failure of most of these services is programmed at birth already, as this closed concept does not allow growth and market penetration, and slows down any effort to reach the critical mass. The network effect is critical in this business, which can only be realized through openness and cooperation. The SEMOPS service is built on cooperation. SEMOPS realised that a successful electronic/mobile payment service needs to assure the cooperation between banks and mobile operators. There were too many attempts on both sides to dominate the business alone without the participation of the other party, but all of them have failed. If participation is limited to a couple of players then huge segments of the population will be left out, the service cannot reach its universal scope.

The SEMOPS service aims to establish the wide cooperation of banks and MNOs along the lines of real financial benefits. It is obvious that the banking sector has different operating specifics from those of the mobile communication sector. It is possible to elaborate an operating structure, where these specifics are combined in a way that results in operating optimum, in terms of efficiency. In the SEMOPS service banks are processing macro and mini payments, while MNOs are processing micro and mini payments. Moreover, for mini payments that are offered by both, the user is the one who decides who to select. This division of work results in substantial cost reduction, risk reduction, utilisation of a joint back end infrastructure and great market coverage. The involvement of a number of the banks and MNOs further increases the market coverage by enabling transactions between any of their clients either on the customer or on the merchant side.

Universality: Most existing mobile payment services are of very specific nature. They are not suitable for micro transactions, or many of them are even more limited scope like payment for digital content, or parking services. Contrary to existing solutions, the SEMOPS service follows a universal approach that aims to both mobile and Internet transactions, it addresses domestic and cross border payments, and it can accommodate various transaction types, irrespective of value, function, time, currency etc. SEMOPS is account based and, therefore, can be used also by people who do not trust electronic card transactions, or for transactions that are of low value and their process is more expensive than the actual value.

Openness: Existing mobile and electronic payment services are rather closed in their structure. The SEMOPS service on the other hand is explicitly open. The service itself is offered to the banks and mobile operators – the payment processors - who are providing the service to their own clients. This approach means that the actual users do not have to centrally register with any third party entity in order to be able to use service. Furthermore there is no centralised authentication, and any client of any payment processor can perform payment to any other client of any other payment processor. When new payment processors joins in the SEMOPS service the potential number of transactions increases rapidly, as all existing SEMOPS users will be able to carry out transactions with clients of the new payment processor.

Independence: Existing electronic payment services are very much technology and operator dependent. The SEMOPS service is independent from technical, operational, and commercial aspects, as it provides a homogeneous layered approach to which components can be exchanged without impact on the other levels. Technical independence means that the service can be used under various technical conditions. There is communication variety, as the payment service is designed to be a used in 2G, 2.5G and 3G, as well as Internet infrastructure. There is platform independence, as there are several front-ends and modules implementations in SIMToolkit, JAVA and OS versions. Independence for the user implies that, even if all components of the service are changed, the service will not be interrupted for both the customer and the merchant. In practice, this means that the user may change country, bank, MNO or mobile device, but still receive the same service, and all the transactions that were available before are still accessible for the users.

State of the art technology: The SEMOPS solution is designed with the state of the art technology in sight. The service utilises protocols like the Bearer Independent Protocol (BIP) when card based solutions are deployed, and MIDP 2.0 when the application is based on J2ME. New APIs like JSR-82 and JSR-120 are also included in the design. The IrDA, Bluetoothand RFID communication in relation with POS technology is also novel, and there are efforts to integrate Instant Messaging approaches as an extension to communication channels in all transactions. The overall design concept that is capable of managing variable communication channels and different security solutions ensures versatility for the service and easy deployment under widely differing conditions. In regards of the back-end infrastructure, the J2EE development integrated with middleware technology provides interoperability. The security services use private/public key pairs for encrypting and signing messages, and we plan also to integrate Elliptic Curve Cryptography (ECC) for better performance on the mobile devices.

CONCLUSIONS

Present electronic payment services are relatively expensive for the users. This is of no surprise if one looks at the operating conditions of the services and the security environment they have to cope with. As discussed in this chapter, the existing services target a limited clientele, they lack scale of economics and, therefore, if they want to be profitable they need to charge hefty commissions. The situation is further deteriorated by the high security expenses and risks these services are facing, either in terms of expensive complex solutions, or high fraud rate, or both.

SEMOPS aims at developing a global mobile payment system with good economical conditions both on the revenue and the cost side. Its innovative business model is based on two key concepts a) that of cooperation of Banks and MNOs and b) that of social trust relationships, since each actor transacts only with his trusted bank or MNO. It is worth noting that SEMOPS features a distributed approach where banks/MNOs can dynamically join the system with their customer base and users do not have to register alone, something which will allow SEMOPS to grow fast and reach a the critical mass that may establish it as a global payment service. In particular, SEMOPS presents the following advantages:

- The service relies on numerous revenue channels and large potential clientele.
- Different sales channels are combined, (Internet, mobile).
- A number of different transaction types are combined, (B2C, B2B, P2P, Escrow).
- Different product categories are combined, (digital content, out of band, vending, gambling, parking, EBPP, traditional products, loyalty programs).
- Various commercial situations are combined, (remote, proximity, POS, P2P).
- The client base of various service providers is combined, (banks, mobile operators, others).

A number of factors contribute to the minimisation of cost of the SEMOPS service. Both capital and operating expenses can be kept at low levels due to the favourable environment and process flow. In particular:

- The service leverages existing infrastructure, especially in the banking environment.
- The service concept is built around the traditional financial processes, modifying them but not completely replacing them.
- The deployment of the necessary technical elements is simple as integration is built on interfaces and middleware technology.
- The use of standardised solutions in the service and in its technical environment further reduces introductory expenses.
- Personnel expenses are low due to the full automation of the service that requires manual intervention only in exceptional cases.
- Communication expenses are low as wherever it is possible the service is optimised to use those communication channels that are the cheapest.
- Risk management, and security expenses are also low, as the service relies on existing risk management practices and due to the trusted feature of the payment process good security protection can be achieved with relatively simple solutions.
- The cost of financial settlement is minimized as transactions are settled in large value batch processes.
- The fact that all different kind/type of transactions are processed on the same back end infrastructures that partially is also shared by other services substantially reduces unit cost compared to any other payment solutions.

Trial SEMOPS services have been deployed in Hungary and Greece. Future plans include extensive cross-border trials and tests, as well as the deployment of a pan-European pilot until 2005.

ACKNOWLEDGEMENT

This paper describes work undertaken and in progress in the context of the SEMOPS (IST-2001-37055), a two-year project (2002-2004), which is partially funded by the Commission of the European Union. The authors would like to acknowledge all SEMOPS partners.

REFERENCES

- SEMOPS (2003), Secure Mobile Payment Service, http://www.semops.com
- Heijden, H., (2002). Factors affecting the Successful Introduction of Mobile Payments Systems. Proceedings of the 15th International Bled Electronic Commerce Conference, Bled, Slovenia, June 17-19th, 2002.
- Henkel, J., (2001). Mobile Payment: The German and European Perspective. In Book: Mobile Commerce, Gabler Publishing, Wiesbaden, Germany. http://www.inno-tec.de/forschung/henkel/M-Payment%20Henkel%20e.pdf
- Kreyer, N., Pousttchi, K., Turowski, K. (2002). Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce. In Bauknecht, K.; Quirchmayr, G.; Tjoa, A M. (Hrsg.): Proceedings of the EC-WEB 2002, pages 400-409, Aix-en-Provence, 2002.
- Mobey Forum (2003). White Paper on Mobile Financial Services, June 2003, http://www.mobeyforum.org/public/material/
- Camponovo, G. & Pigneur, Y. (2002). Analyzing the Actor Game in m-Business. First International Conference on Mobile Business, Athens, Greece, 8-9 July 2002. http://inforge.unil.ch/yp/Pub/02-Athens.pdf
- Pfitzmann, A., Pfitzmann, B., Schunter, M., and Waidner, M (1999). Trustworthy user devices. In Günter Müller and Kai Rannenberg (editors), Multilateral Security in Communications, Information Security, pages 137-156. Addison-Wesley, 1999.
- Karnouskos, S., Vilmos, A., Hoepner, P., Ramfos, A., Venetakis, N. (2003). Secure Mobile Payment - Architecture and Business Model of SEMOPS. EURESCOM summit 2003, Evolution of Broadband Service, Satisfying user and market needs, 29 Sept - 1 Oct 2003, Heidelberg, Germany.
- Vilmos, A. & Karnouskos, S. (2003). SEMOPS: Design of a new Payment Service. International Workshop on Mobile Commerce Technologies & Applications (MCTA 2003), In proceedings of the 14th International Conference (DEXA 2003), IEEE Computer Society Press, pages 865-869, September 1-5, 2003, Prague, Czech Republic (ISBN 0-7695-1993-8).