SEMOPS: PAYING WITH MOBILE PERSONAL DEVICES

A. Ramfos [a], S. Karnouskos [b], A. Vilmos [c], B. Csik [d], P.Hoepner [b], N. Venetakis [a]

[a]Intrasoft International, Athens, Greece, www.intrasoft-intl.com

[b]Fraunhofer Institute FOKUS, Berlin, Germany, www.fokus.fraunhofer.de

[c]SafePay Systems, Budapest, Hungary, www.safepaysys.com

[d]Profitrade, Budapest, Hungary, www.profitrade.hu

Abstract: The growth of mobile commerce is directly related to the increase of ownership and use of mobile personal, programmable communication devices, including mobile phones and PDAs. These devices provide effective authorisation and management of payment and banking transactions since they are capable of offering security and convenience advantages compared with existing methods, such as credit/debit card transactions and online payments through a PC. Some of these advantages are part of the existing devices' functionality while others require modest, inexpensive enhancements likely to be incorporated in the mobile devices to come. It is expected that the use of secure and convenient mobile personal devices can revolutionise the payment, banking and investment industries worldwide. This paper presents SEMOPS, a secure mobile payment service implemented on innovative technological solutions and introducing a competitive business enabler of mobile commerce. SEMOPS intends to exploit the business opportunities inherent in the billing, customer-service, technical relationships and banking services among mobile customers, mobile operators and banks in order to offer a competitive solution to existing payment services.

Key words: e-commerce; m-commerce; e-payment; m-payment; security

Fourth IFIP Conference on e-Commerce, e-Business, and e-Government (I3E), 22-27 August 2004, Toulouse, France.

1. 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 [3]. 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, including the compromise of the bank's computers or, in the case of online banking, 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 [5]. Mobile personal devices provide a technical solution for personalised I/O interface to payment transactions since the transaction initiator is the owner of the mobile device also. 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.

Several mobile payment systems have been realised as prototypes or even as commercial products, however none of them managed to establish itself as a global mobile payment service. There have been several criteria on the technology side and on the business model that have restricted the capabilities of such procedures. SEMOPS features an extensible business model that takes advantage of the legacy infrastructure and its trust relationships, and also tackles privacy. Furthermore, most existing payment procedures today can satisfy a limited number of scenarios such as Top-Ups, mTicketing or P2P payments, but with sometimes complex procedures, not cost-effective solutions and limited applicability. The SEMOPS approach is more general, can be easily extended to integrate any third party financial service provider and is suitable for any payment scenario, even for cross-border ones. This paper will provide an insight on some design and implementation decisions of SEMOPS and we will balance this with the commercial viewpoint of the approach.

2. MOBILE PAYMENT SOLUTIONS

Figure *1* outlines a typical mobile payment transaction. This modular transaction architecture can be used for multiple applications and scenarios. The simplest scenario involves only the user, the device and a single payment processor, such as a mobile operator, bank, credit card organisation, broker or an insurance company. The user identifies 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, and, then, the two payment processors have to be able to interoperate.

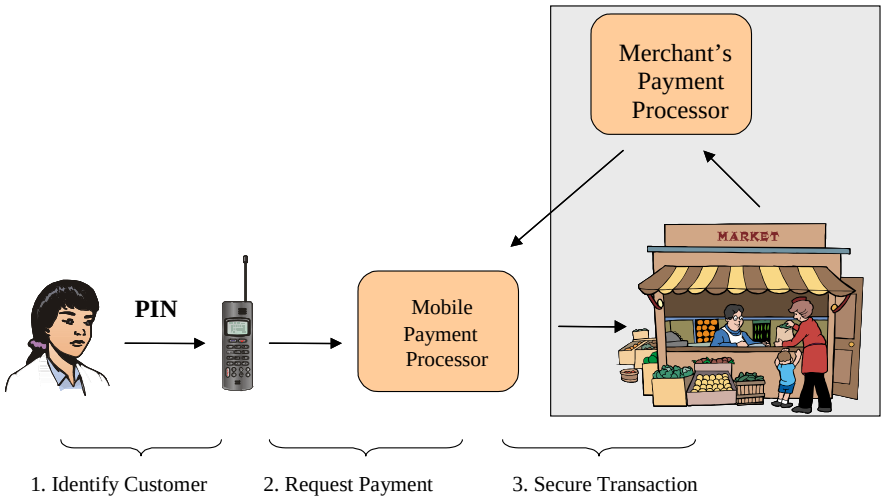

Figure 1 – Mobile Payment Transaction

Most of the existing mobile payment solutions assume that a mobile payment service is offered to the customers of a particular mobile network operator (MNO), as shown in Figure 2. These payment solutions allow customers of a particular mobile operator to perform payment transactions with merchants who are contracted by the same MNO. 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 a limited number of existing payment solutions have the capability to reach the critical mass for the adoption of mobile commerce, they offer limited transaction potential and limited accelerator effect of mobile commerce [2].

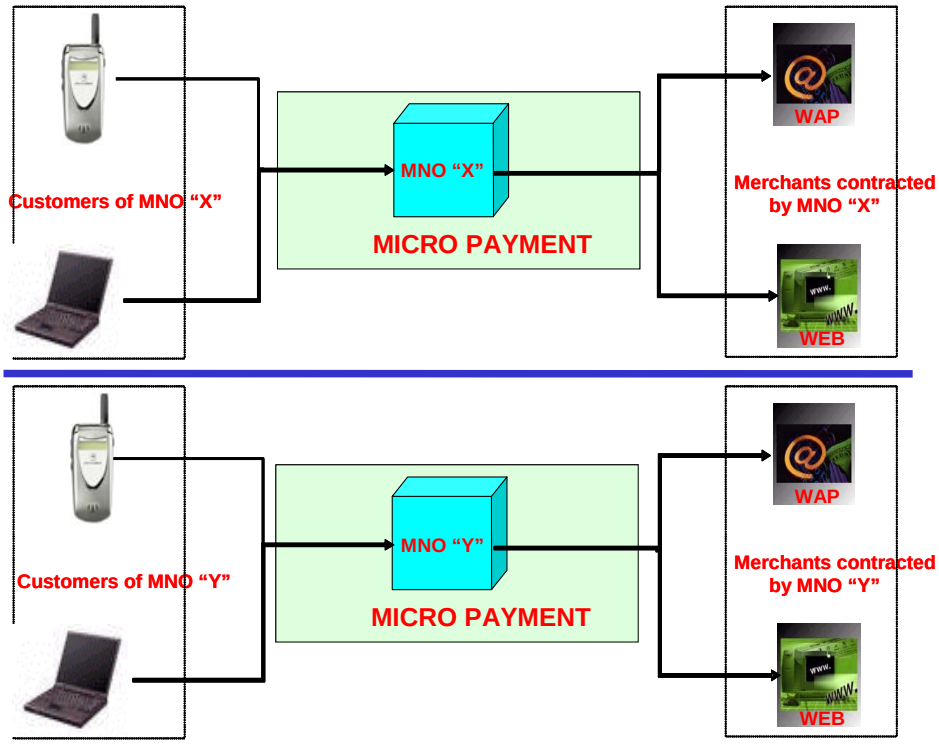

Figure 2 – Existing m-payment solutions

In this paper, we present SEMOPS [1] 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 *3*, 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 [4].

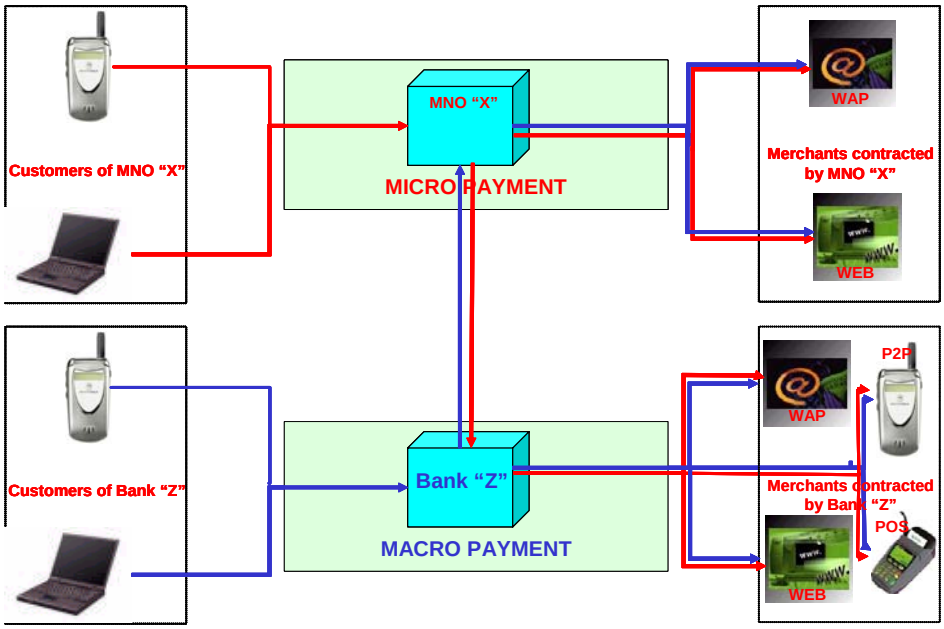

Figure 3 – SEMOPS m-payment solution

As shown in Figure 3, 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.

3. SEMOPS TRANSACTION ARCHITECTURE AND FLOW

As in every payment system, the aim of SEMOPS is to transfer funds from the customer to the merchant, or, in more general terms, from the payer to the payee. The SEMOPS payment solution, however, is novel in that it establishes a process flow that allows cooperation between banks and mobile

operators. Figure *4* gives a view of the modular architecture of the SEMOPS payment solution in which the payer and the payee exchange transaction data, while the fund transfer is done via trusted payment processors, the customer and merchant banks, respectively. Each user (payer or payee) connects with his home bank/MNO only. The banks exchange messages between them via the Data Center (DC). The legacy systems of the bank and of the merchant are integrated in the SEMOPS infrastructure and are used as usual. 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.

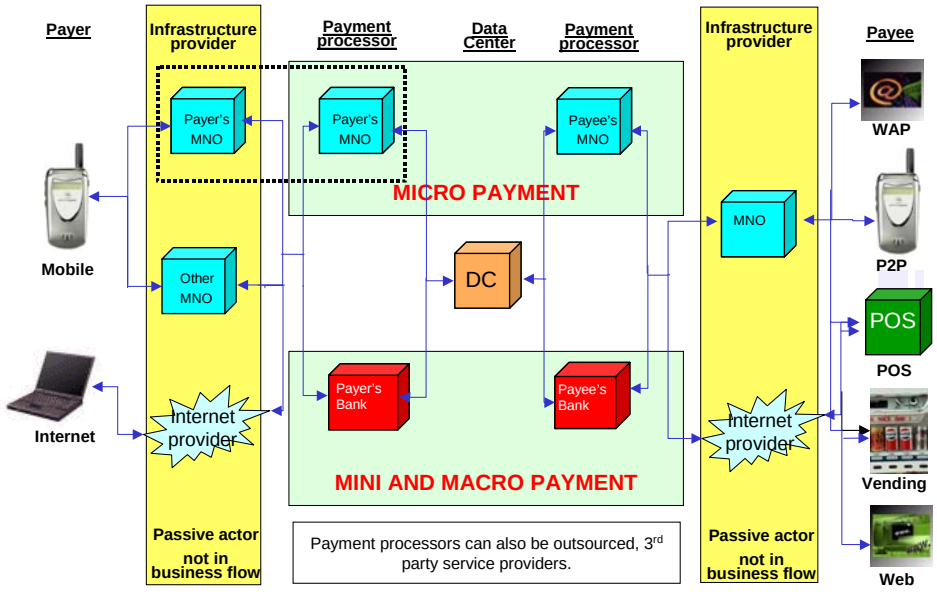

Figure 4 - Overview of SEMOPS payment network architecture

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 presented in the following, (see Figure *5*):

- 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 provides 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.

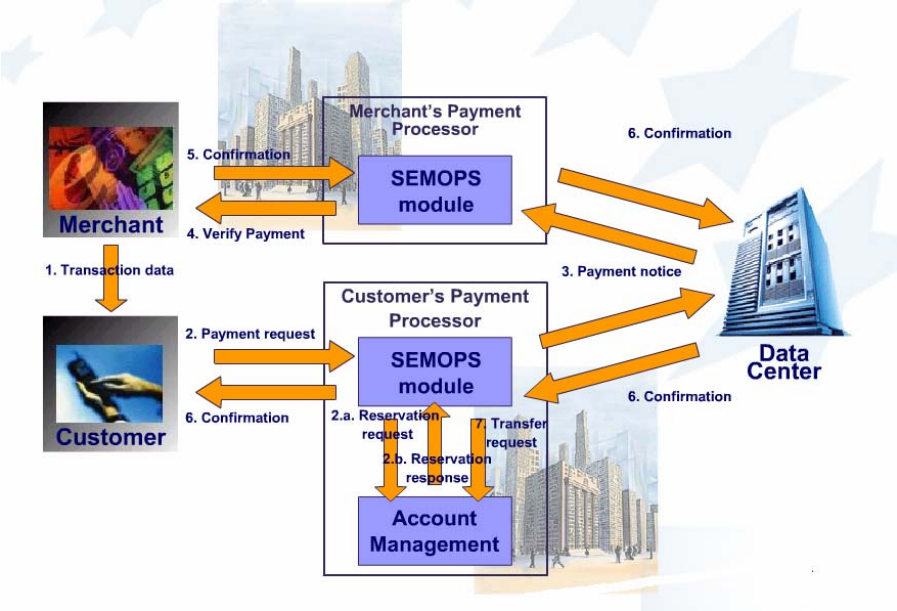

Figure 5 – SEMOPS Transaction Architecture

The above-mentioned description refers to a prompt payment. However, the SEMOPS solution is more versatile and allows also deferred, value date and recurring transactions. SEMOPS supports a refund feature as well, and in case of cross border transactions conversion between currencies is also possible.

Should for whatever reason the transaction is not completed, , the customer's payment processor releases the funds it has reserved for the purchase. The following reasons could cause disruption to a transaction:

- The customer may use a wrong PIN while requesting payment
- Not enough funds are available on the customer's account
- The merchant may reject the transaction
- Communication problem

4. SEMOPS SYSTEM TECHNICAL 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 with 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.

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.

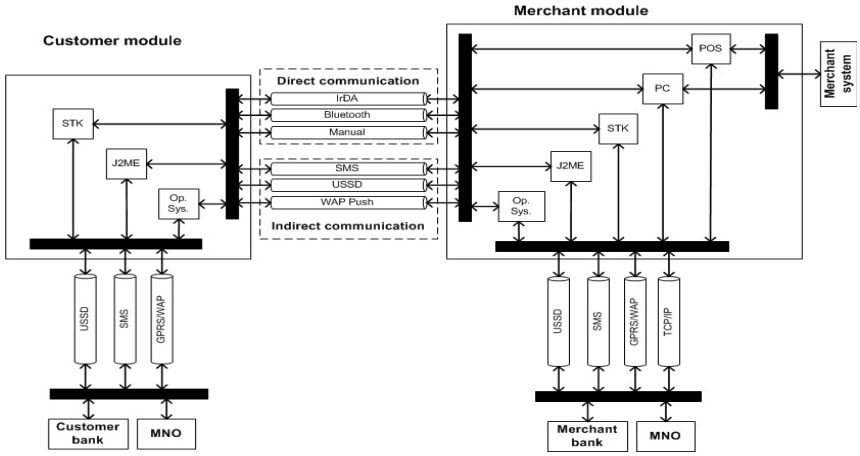

Figure 6 - Base Technologies of Front-End Modules

As shown in Figure 6, 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.

4.1.1.1 Customer Module

The customer module 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. There are three basic features in all types of customer modules, i.e., personalisation, payment processing and transaction management. The personalisation features allow high-level usability and convenience for the users. 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 module allows storing of all user related, non-sensitive information that is frequently used. It also enables storing multiple user and payment processor profiles, in order to let the user choose her preferred payment processor for each individual transaction. All information can be password-protected, and the protection level is also adjustable by the customer. 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. Transaction management includes a wide variety of functions that are related to the handling of the stored transaction information. Besides providing historical information about past purchases, certain manual transaction types, refund requests and synchronization commands can also be launched using the administrative functions.

4.1.1.2 Merchant Module

The merchant module 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. Similarly to the customer module, all permanent information can be safely stored, minimising the data amount that needs to be transferred between systems or input manually. During the payment transaction the merchant module communicates with the customer and transfers all the information necessary for completing the payment. 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.

It can be clearly seen from Figure 6 that the SEMOPS solution achieves the widest technology coverage in terms of:

- The platform of the customer module
- The platform of the merchant module
- The merchant – customer communication channel
- The customer – customer Bank communication channel
- The merchant – merchant Bank communication channel

5. DESIGN AND IMPLEMENTATION CONSIDERATIONS IN SEMOPS

The design of the system is open and flexible for future integration of hardware and software modules, as well as cooperation with other applications and services.

In order to accommodate the heterogeneity of supported mobile platform in SEMOPS front-end modules (STK, J2ME, other platforms), all front-end modules' design share common UML Use Case models and Activity Diagrams. After achieving this common design base for all front-end modules, operating platform-specific designs were produced, (depicted in Figure *7*).

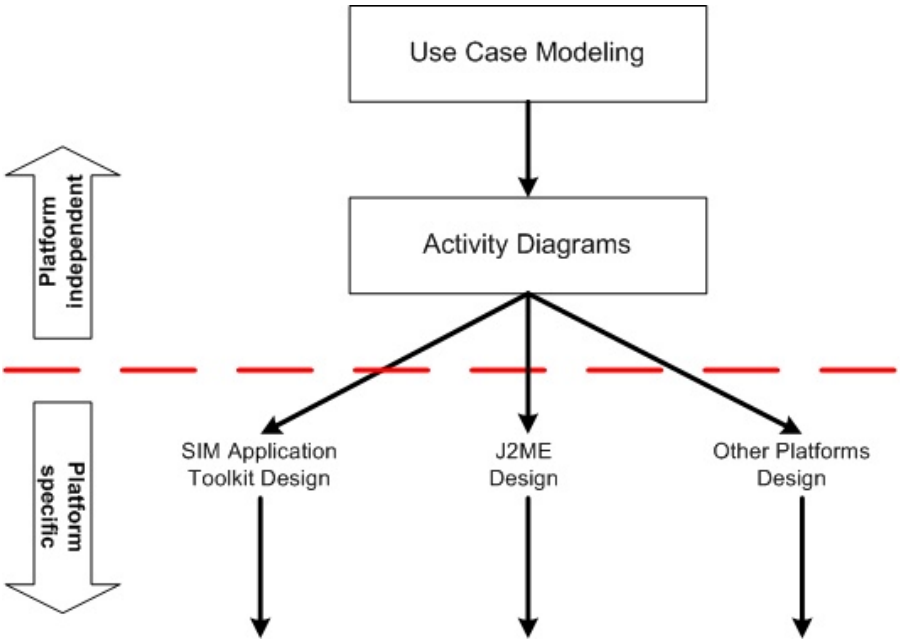

Figure 7 - Overview of the mobile module designs

From these operating platform-specific designs, the SIM Application Toolkit one is the most unique, since the design steps are a mixture of the RUP/UML methodology and the procedural system design. Due to the limited storage and process capabilities of SIM cards, the application was decomposed into re-usable components in order to achieve an efficient storage management within the inherent SIM cards storage limitations.

The software implementation environment of the SEMOPS solution consisted of: Java2 (J2EE/J2ME), XML, ORACLE9i, and WebSphere v5.1

6. SECURITY IN SEMOPS

SEMOPS provides a strong end-to-end encryption for transferred data and allows the usage of different authentication techniques embedded into this encryption. SEMOPS built up its security framework with the following considerations:

- Banks do not allow encrypted information into the Intranet: Decryption must be done in the Demilitarised Zone (DMZ).
- Banks usually have their own authentication system already: SEMOPS must co-operate with existing authentication facilities.
- SEMOPS uses heterogeneous channels, e.g., TCP/IP, GPRS, SMS, USSD: SSL cannot be used as encrypted channel.
- Different country regulations prohibit the usage of the same keys for encryption and signing: SEMOPS works with multiple key pairs.

Based on these considerations, SEMOPS utilises the security model depicted in Figure 8. The termination of the physical channels and the decryption of the messages occur in the DMZ. The decrypted information reaches the SEMOPS Bank Module (residing on the Intranet of the bank and implementing the core business logic) through the bank's standard authentication system, which is already used for applications, like home banking. Currently SEMOPS uses 1024 bit RSA encrypted XML with 3DES message keys, and also uses 1024 bit RSA digital signatures on the messages, but with a different key pair. The security modules execute all the cryptographic operations in the system, resulting in the split security operations depicted in Figure *8*.

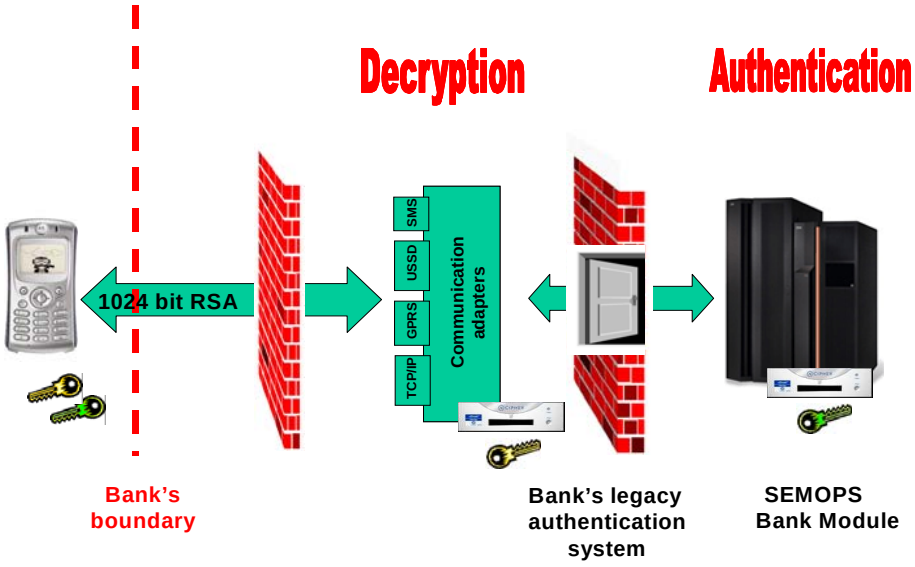

Figure 8 – SEMOPS Security Infrastructure at Payment Processors Site

7. CONCLUSIONS

SEMOPS realises a secure mobile payment solution, which is capable of electronic and mobile commerce scenarios. The SEMOPS approach can also accommodate anonymous payments, which is something that can be done only with cash today and limited prepaid money-token cards. Both, modules that interact with payers and payees (front-end modules) and modules that interact with payment processors' systems (back-end modules) are designed to have extended functionality, security, openness, usability and a versatile application-executing environment. In particular, SEMOPS front-end modules are very versatile from the mobile technology point of view and combine all viable implementation possibilities in user-processes and mobile/Internet technologies. Its design enables the cooperation of banks and MNOs in providing a trusted and convenient mobile payment service. The payment processors in the SEMOPS service can be any combination of banks and MNOs, and each actor in the service, either payer or payee transacts only with his trusted bank or MNO. SEMOPS covers both mobile and Internet transactions, addresses domestic and cross border payments, and can accommodate various transaction types, irrespective of value, function, time, currency etc. It is worth noting that SEMOPS features a distributed approach where banks and MNOs can dynamically join the system with their customer base, something that will allow SEMOPS to grow fast and reach a critical mass that may establish it as a global payment service. 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) [1], 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

[1] Secure Mobile Payment Service (SEMOPS), http://www.semops.com

[2] "Mobile Payment: The German and European Perspective", Joachim Henkel, G. Silberer (ed.): Mobile Commerce, Gabler Publishing, Wiesbaden (2001).

[3] Mobey Forum White Paper on Mobile Financial Services, June 2003, http://www.mobeyforum.org/public/material/

[4] "Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce", Kreyer, N.; Pousttchi, K.; Turowski, K. In: Bauknecht, K.; Quirchmayr, G.; Tjoa, A M. (Hrsg.): Proceedings of the EC-WEB 2002, Aix-en-Provence, 2002.

[5] "Trustworthy user devices", Pfitzmann, A., et al: Multilateral Security in Communications, G. Muller and K. Rannenberg, Eds., Addison-Wesley, 1999, pp 137-156