12

Instant Messaging Enabled Mobile Payments

Stamatis Karnouskos, Tadaaki Arimura, Shigetoshi Yokoyama
and Balázs Csik

12.1 Introduction

12.1.1 Mobile Payments

According to an old telecom saying, no service can be considered as such, unless you can charge for it. Mobile payment (MP) is a term used to describe any payment where a mobile device is used in order to initiate, activate and/or confirm this payment. Contrary to popular belief, mobile payments do not restrict themselves to payments via mobile phone but can be made by virtually any mobile device such as Tablet PCs, PDAs, Smartphones, or even merchant-operated mobile terminals. Several approaches have been developed [1–4], but up to now none of them has managed to reach the critical mass and establish itself as a global mobile payment service. The availability of such a service will be a driving force for the development of new mobile applications, will accelerate the growth of mobile commerce, will generate new business opportunities for the mobile operators and as such will contribute to the overall economic growth [5]. Several institutions predict that, in the next few years, payment by mobile phone will become common. [1, 6]. Some go even further, naming MP as the future killer application for mobile commerce in a 2.5 G and beyond infrastructure. Mobile Payment is expected to boost both m- and e-commerce as users will be able to pay for e/m content, in vending machines, use m-ticketing, reload their prepaid cards Over the Air (OTA), do m-shopping and pay in real and virtual Points of Sale (POS).

With today's mobile and wireless networking technologies such as GPRS, UMTS and WiFi, the Internet and its services are available to almost any kind of end-device. It is therefore an evolutionary step that many applications undertake, appearing in a mobile version that takes into account the limitations set by the end-devices such as memory, speed, capacity and connectivity. Most of the mobile payment approaches try to use widely available phone features in order to address a wide customer base. Therefore, most of them are based on SMS, but some use a combination of SMS and IVR (Interactive Voice Response) for user authentication. Some more advanced approaches take into account the last technical developments in mobile devices and make use of protocols such as IrDA and Bluetooth, while

Emerging Wireless Multimedia Services and Technologies Edited by A. Salkintzis and N. Passas

others even use existing execution environments such as JAVA and data connections such as GPRS, EDGE, etc. The debut of UMTS, wireless LAN, WiMAX and other 3G and beyond technologies will provide new capabilities [7] that will free MP from some of its limitations and allow more sophisticated approaches to be developed. In such an infrastructure, data services will become more important and provide the real revenues for the Telecom operators and their partners. Even the voice, the killer application for existing mobile phones, is going to be data based and replaced by Voice-over-IP (VoIP).

Moving towards all-IP networks means that applications and services over mobile devices will increase in number and importance, and the demand for a method of paying for them will be evident. Strict telecom billing (e.g. via the mobile phone bill or as a prepaid amount) is only one of the approaches that fail within the mobile payment domain. Mobile network operators (MNO) can handle micro-payments (usually amounts under $2) and mini payments (usually amounts ranging from $2 up to $20). Although this can provide some flexibility, we need to cover also a wider spectrum on payment amounts and, for that, the help of banks and third party financial service providers (e.g. credit card organizations) is needed. They could successfully handle mini payments, but also cover macro payments (typically any amount above $20). So, as we can see, there is a need to develop approaches that will provide a global mobile payment service that has the right business model and simultaneously takes advantage of the infrastructure and capabilities that will be common within the next years.

In the mobile payment domain, many standardization organizations and consortia [1] are working towards the goal of finding the right approach. In general, we can distinguish the following categories in existing consortia.

- MNO driven. Simpay (www.simpay.com), Starmap Mobile Alliance, GSM Association (www.gsmworld.com), European Telecommunications Standards Institute (ETSI – www.etsi.org), Universal Mobile Telecommunications System forum (UMTS – www.umts-forum.org).
- Bank driven. Mobey Forum (www.mobeyforum.org).
- Cross industry driven. Mobile Payment Forum (MPF – www.mobilepaymentforum.org), Mobile Payment Association (MPA – mpa.ami.cz), Paycircle (www.paycircle.org).
- Device manufacturer driven. Mobile Electronic Transactions (MeT – www.mobiletransaction.org).
- Technology driven. Open Mobile Alliance (OMA – www.openmobilealliance.org), Infrared Data Association (IrDA – www.irda.org).
- Identity driven. Radicchio (www.radicchio.org), Liberty Alliance (www.projectliberty.org).

We can clearly see that there is a lot of interest in mobile payments and, although there are some successful and promising approaches, there is still a long way to go before we can realize a global mobile payment service that will empower future mobile and electronic applications.

12.1.2 Instant Messaging

Instant messaging (IM) is a widely used service in fixed Internet infrastructure. Successful examples include ICQ (www.icq.com), Microsoft MSN Instant Messenger (messenger.msn.com), Yahoo! Instant Messenger (messenger.yahoo.com) and AOL Instant Messenger (www.aol.com/aim). Standardization fora and consortia have been working on interoperable instant messaging and presence protocols such as the SIMPLE [8], XMPP [9] and the IMPP [10] of IETF (which has become more of a standard that encompasses SIMPLE and XMPP). IM enables online users to check the status of people in their contact list and send messages in real time to each other. Therefore, any IM approach deals with synchronicity and presence awareness. The infrastructure follows the client-server architecture where the IM application is stored on the client and connects to a server in order to request the presence status of specific users. By making such a service available to mobile users, the 'anytime, anywhere' flexibility of mobility could make the already highly popular IM even more widely used, and new kind of applications can be developed that will rely on IM as an underlying message carrier. It is predicted [7]

that by 2005 the revenue from mobile instant messaging in Europe could be as high as 760 million euros. Existing efforts support near real time message distribution in one-to-one or one-to-many connections. Mobile IM is one of the first presence enabled applications and, although it is basically used for transmitting text messages, it can be used for transmitting images and support multi-user applications such as shared content, white-board, conferencing, etc. Instant messaging should not be seen as a standalone service. In any future mobile scenario, context awareness sets an important new paradigm [11]. The majority of context aware applications nowadays focus on location awareness, therefore instant messaging should also be seen in that context, and especially coupled with the concepts of presence and location. This integrated approach is expected to empower future personalized mobile Internet applications that will adapt themselves to the current user's context. By adding mobile payment, it will be possible to enrich the polymorphism of such services but also their attractiveness since a personalized payment function is there. Open standards for Mobile instant messaging have been defined by the Wireless Village initiative and Open Mobile Alliance (OMA) [12] and mobile phones with integrated IM clients are already on the market.

12.1.3 Instant Messaging Enabled Mobile Payments (IMMP)

As we have mentioned, both instant messaging and mobile payment are promising approaches in their respective domains. Combining both of them would create a powerful duo that we consider needs to be further researched. Existing mobile payment approaches use SMS, IrDA and Bluetooth for communication. SMS has been proven to be not only insecure and unreliable, but also expensive. Therefore it may suit any archaic efforts on MP, but definitely cannot be used neither for macro payments (for security reasons) or for mini/micro-payments (due to its high cost). IrDA and Bluetooth are two protocols that require either a line of sight between the transacting devices or a limited distance between them, therefore they demand that both transacting partners in a payment scenario are more or less in the same physical space. It can be clearly seen that IM could easily slip into the role of any of these protocols. It can support security (that can be embedded on the application) and can be cost effective, since there is data communication. Furthermore both transacting parties do not necessarily have to be in the same physical space. Therefore, IM can generally replace all the aforementioned protocols in any mobile payment scenario.

However, taking a closer look at it we can see that (i) IM is a suitable medium for real-time communication, and (ii) it can be personalized based on our current context. Therefore it makes sense to use IM in mobile payments, especially within the context of person-to-person (P2P) mobile payments where both parties are known to each other (e.g. belong to the 'buddy' list). In this chapter we take this as a use-case and explore how such a service can be designed and implemented.

12.2 An Instant Messaging Mobile Payment Scenario

It is already 2008, the technology world has survived the. com crash and investments on technology related areas have started increasing again. Internet based services are flourishing, however they are not alone this time. Mobile services are also gaining momentum and, due to their nature (anywhere, any time, in any form), have far outrun their Internet siblings in some sections. People no longer have to go home and log into a terminal to do their job; the mobile city vision has successfully made its first steps and a wide variety of people, ranging from youngsters who simply want to try the latest mobile games to business professionals who travel around the globe and want to know in real-time their portfolio performance at the stock exchange, constitute a large diverse clientele for the mobile service market. In such an era where the mobile services are starting to become integrated into the tasks of everyday life, payment for such services is a must. The mobile services and the user have set demanding requirements such as real-time payment processing and interaction with a wide variety of virtual and real points of sale around the world in virtually any currency. The good news is that this trend has been recognized

early enough and such global payment services exist. In 2008 mobile payments are not only possible, but form a generic service that other more intelligent services in e- and m-commerce can easily integrate and with which they can interact.

Evelyn is a child of this era and, although she is only twelve, she has been a mobile phone owner for many years and really cannot imagine how people had managed their daily life before mobile phones. Having finished her school day, she is on her way back home, when she passes through the shopping center. Her phone beeps; a new notification has arrived from her favorite toy store (which thanks to location based services has noticed her presence) that just for today the doll that Evelyn wanted is reduced in price by thirty percent, a special discount for her as a loyal customer and, of course, as gift for her upcoming birthday. Evelyn cannot really believe her luck. She immediately looks at her instant messaging tool to see if her father or mother are online, and ask them if she can buy it. Yes, her father who is currently on a business meeting abroad is online. She quickly drafts an instant message to him, informing him of the discount and adding a photo of the doll, just to encourage his approval. Some seconds later her father replies, 'OK, go ahead sweetheart. I was planning to get this tomorrow, but you can have it today if you want'. Evelyn lets the store personnel pack the doll and is ready to pay. She can't pay with real cash as the doll costs much more than the money she carries on her or the money stored in her phone, and she is too young to have a credit card. However, this is not a problem today as her father can authorize the payment sent from the store, via his mobile from anywhere in the world although he is not physically with her. Evelyn's father receives a signed instant message from the merchant (directly or duly forwarded from Evelyn) containing an invoice for the purchase his daughter is making with her mobile phone. Subsequently he authorizes the payment and a real time receipt arrives not only at his mobile phone, but also at his daughter's and with the merchant. The transaction is complete, the doll is paid for and Evelyn can now leave the store with her birthday present. Evelyn's father knows that since he subscribed to this service he has made his family life easier by being able to handle similar situations while being mobile. The happy smile on the face of his loved ones and the easie and flexibility that this has brought to his everyday life is the reason why he keeps subscribing and, frankly, he also considers it strange that once such a service only a vision.

12.3 The Generic MP and IM Platforms of IMMP

Developing an IMMP approach from scratch would be like reinventing the wheel, especially when there are already prototypes available that can be brought together. Therefore we have concentrated on sticking together two existing approaches by creating the necessary APIs and the message exchange via which the two systems could cooperate. We have therefore chosen the Secure Mobile Payment Service (SEMOPS [13]), an innovative mobile payment service prototype, and the Air Series, a mobile IM service [14]. The authors of this chapter were active participants in the development of these two prototypes, so our work in trying to define the common APIs and integrate the systems was eased. In order to better facilitate our dilemmas in the design of the IMMP, we give a short introduction to these services and the way that they operate. The same operation and functions are also available on the integrated version of these two, namely the IMMP.

12.3.1 The Secure Mobile Payment Service

SEMOPS was initiated with the aim of effectively addressing most of the challenges bundled with a mobile payment service, and developing an open, cross-border secure approach [15]. The service is built on the credit push concept and is based on the cooperation between banks and mobile network operators (MNO). An innovative business [16] model that allows revenue sharing is combined with state of the art mobile technology with the goal of developing a real time, user-friendly mobile payment service, for virtual and real points of sale (POS), as well as for person-to-person transactions. The solution establishes new ways of interaction between the mobile commerce players, thereby relying on the

already established traditional trust relationships between customers/merchants and their existing home bank or MNO.

The aim is to combine the new payment solution with various forms of proven and state-of-the-art mobile and wireless technology in order to achieve a high level of security, availability, user friendliness and interoperability. We have therefore taken into account existing approaches and, after evaluating them, an architecture that overcomes the already identified problems was designed. As in every payment system, the aim is to transfer the funds from the customer side to the merchant side. This usually happens via a financial service provider such as a bank. Figure 12.1 shows a simplistic view of what a global MP is targeting. The developed service [17] wants to provide a secure global payment service that will accommodate a wide range of sophisticated functions and basically will compete with the use of cash payments as we know today. The merchant and the customer exchange transaction data and then the fund transfer is made via the trusted payment processor (in Figure 12.1 it is the bank). The DataCenter simply routes the information flow between the actors.

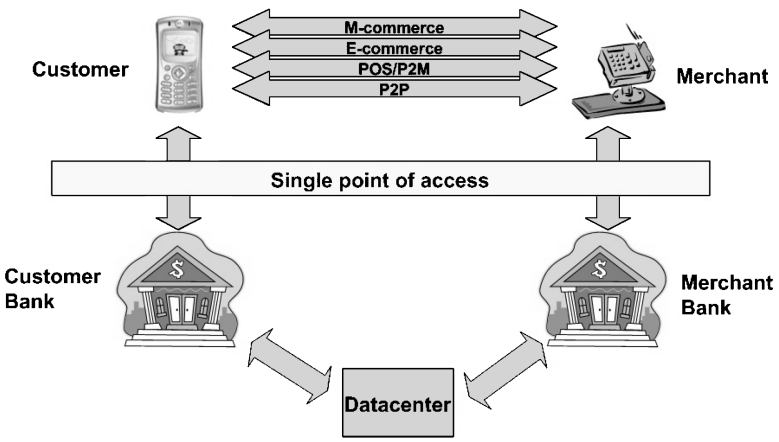

Figure 12.1 Overview of MP concept (bank-based model).

The proposed mobile payment service is based on the structured interaction of individual modules as can be seen in Figure 12.2. There are different transaction and channel specific front-end modules developed to reflect the underlying dependencies in heterogeneous environments and to provide a user-friendly interaction. In the mobile environment the customer modules are tailored to the specifics and technical quality of the handsets, as the design contains not only the SIM toolkit based applications but also the more modern Java and OS based modules. The payment service developed is novel in the sense that it establishes a process flow that allows cooperation between banks and mobile operators or, in general any other third service providers that can slip into these roles, e.g. a financial service provider that can assume the tasks of a bank.

In Figure 12.2 one can distinguish the main players and components in a mobile payment scenario. Each user (customer or merchant) connects with his home bank/MNO only. The banks can exchange messages between them via the Data Center (DC). We should mention that the legacy systems of the bank and the merchant are integrated in the proposed infrastructure and are used as usual. In order to give an idea of the interworking of the approach we describe one of the possible scenarios.

(1) The merchant (in general any realPOS/virtualPOS) provides the customer with the necessary transaction details. This is generally done via SMS, IrDA or Bluetooth.
(2) The customer receives the transaction data and subsequently initiates the payment request, authorizes it and forwards it to his payment processor (at the customer's bank or MNO).

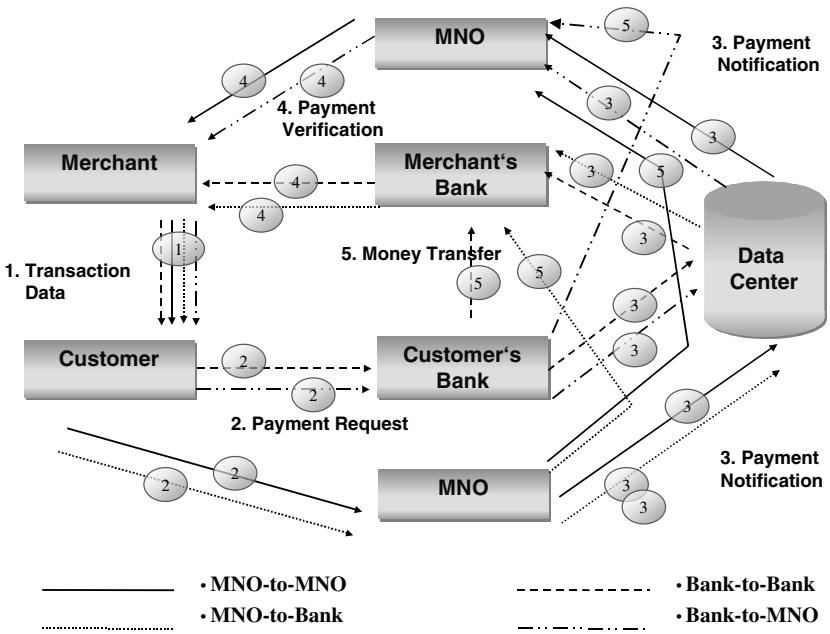

Figure 12.2 High-level information and money flow.

(3) The payment processor identifies the customer, verifies the legitimacy of the payment request and forwards this request to the merchant's payment processor via the DC.
(4) The merchant's bank receives the payment notice, identifies the merchant and asks him to confirm or reject the transaction.
(5) Once the merchant side confirmation comes, the funds transfer is made and all parties are notified of the successful payment.

The description above refers to a prompt payment, and is a fraction of the area covered by the MP service. However, the service is more versatile and also allows deferred, value date and recurring transactions. The service also has a refund feature and, in case of cross border transactions, automatic conversion between currencies is also possible. Further information on the architecture, design and economics of the approach can be found in the authors, previous work [17].

12.3.2 Air Series Wireless Instant Messaging

The Air Series wireless instant messaging [14] is a platform developed for deployment as an added value service for mobile users, and to aid the later introduction of more sophisticated context aware services. As expected, it can offer all of the capabilities of an IM platform and is purely Java based on the server and client side.

Three different parts have been developed, namely the Air Messenger client software, the AirBridge (a gateway for communication protocol conversion), and the AirBOT (an agent like application development framework), all of which compose a fully mobile messaging solution. Taking advantage of instant messaging technology, it is possible to go beyond today's Web services for mobile terminals, and develop more interactive and real-time services, one of which could be mobile payments. Figure 12.3 depicts the overall architecture of the Air Series IM solution. One can clearly see the technologies and modules of the architecture, the major ones are described below.

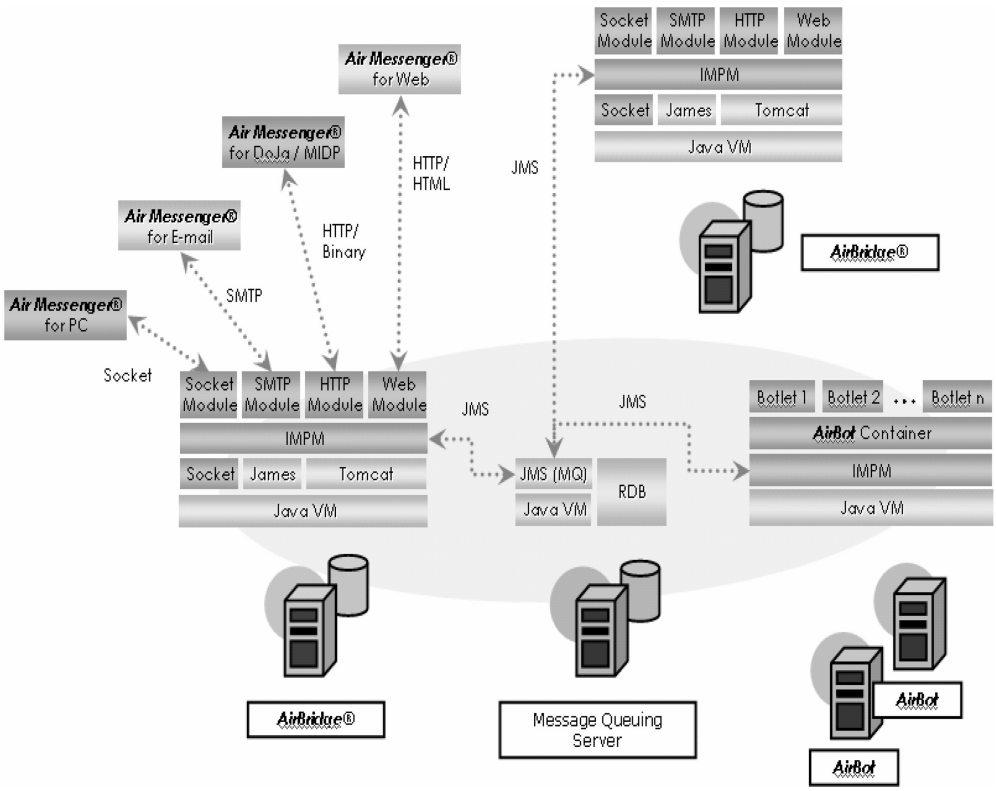

Figure 12.3 The IM platform architecture.

- The AirBridge is a module that provides a robust and reliable framework for message and presence exchange, and seamlessly connects PCs and mobile terminals over unstable wireless connections. As depicted in Figure 12.3, the communication modules are located on the front-end of the server and handle protocol translation. For instance, when a sender sends an SMTP-based message to a receiver using HTTP-based AirMessenger, the message is forwarded to the HTTP module which compresses it to binary formats (which may be device or application dependant) for transmission efficiency. In addition to this, each module is also responsible for delivery or read-reply report management. The IMPM is a core API library to provide IM services such as messaging, presence management, and contact list management. IMPM also controls sessions between the Message Queuing Server and communication modules. Each communication module utilizes these APIs and communicates with others via the Message Queuing Server.
- The Message Queuing Server provides message queues of each user's messages. Because wireless/ mobile connections are periodically unstable, messages are often lost or resent. In order to address this unreliability problem, AirBridge uses the message queuing function of the server to reliably send messages to clients.
- The AirBOT is an application development framework for IM based real-time, agent-enabled service called BOTlet. With AirBOT, developers can easily build BOTlets on their framework and extend IM functionality from a simple messaging function to an advanced application. On the AirMessenger, entries of the AirBOT agent are listed along with 'buddies' in the contact list and users can talk with them just as they do with their friends. Answering questionnaires or information retrieval are examples of AirBOT enabled services.

In general, any HTTP/Socket/Mail based client application communicates through AirBridge with the IM server which is based on the Java Message Service (JMS) [18]. The AirBridge development has taken into account the work done in standardization fora such as the Wireless Village and relevant technologies such as SIP/SIMPLE [8] and PAM4.0 [19]. However, in the prototype a proprietary protocol is also used, in order to enhance the functionality of the IM platform and the AirBot.

12.4 Design of an IM-enabled MP System

We have designed and implemented a prototype of IMMP for wireless/mobile devices. IM in this context is used as an additional channel in order to allow the transacting parties in a mobile payment scenario to initiate contact and exchange data that will lead to the realization of the payment process. Although many existing communication aspects within the existing flow [17] can be performed via IM, we consider IM as most appropriate for the front-end communication, i.e. that of customer and merchant between themselves (peer-to-peer) and their respective banks. The payment process starts with the merchant side providing the transaction data to the customer, which is bundled into a transaction data message according to the specifications [13]. This initial step can be done via IM, especially in cases where the customer and the merchant are not in the same physical space, e.g. Internet purchases.

Basically, our goal was to integrate two different components, one that has been developed to handle the mobile payment transaction (semops) and the other that will provide the add-on functionality of instant messaging. This integration can be done in different ways according to the location and degree of integration between the two components. Each approach has its own pros and cons. In general, we considered the following possibilities:

- the server-based approach (Figure 12.4);
- the 'cooperating clients' approach (Figure 12.5);
- the integrated module approach (Figures 12.6 and 12.7).

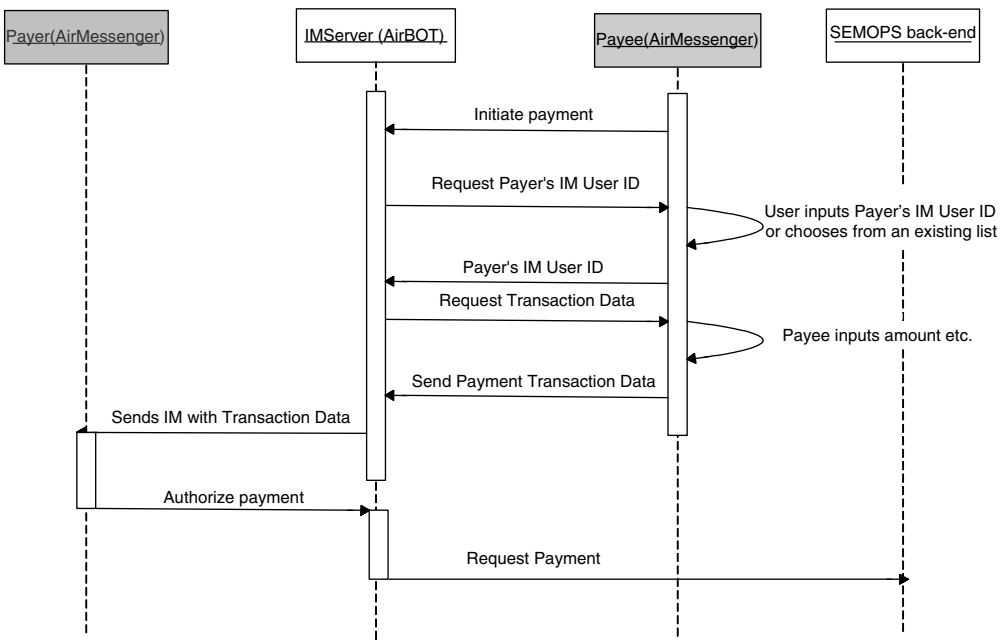

Figure 12.4 P2P payment process (server-based).

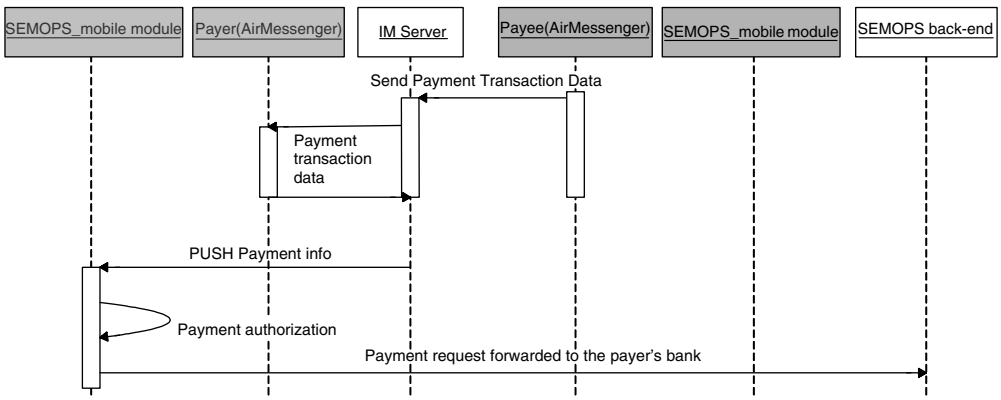

Figure 12.5 P2P payment with 'cooperating clients'.

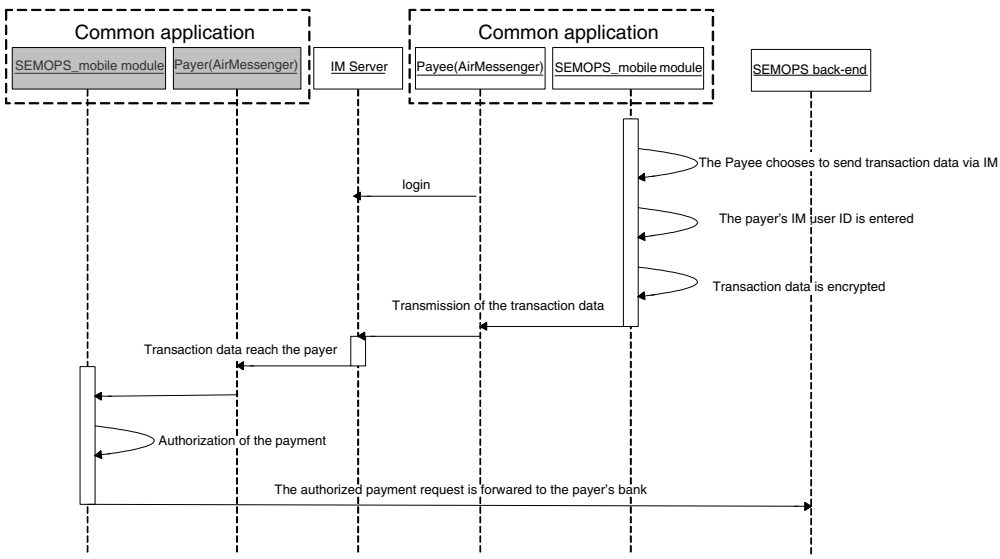

Figure 12.6 Integrated Module approach (MP front-end).

The grey-shaded boxes in Figures 12.4–7 reside on the mobile device of the customer while the dotted-shaded ones reside on the mobile device of the merchant. The remaining components are hosted on the service provider side and are expected to be connected via the Internet. The following sections provide an insight into some possible implementation approaches when one has two independent components (in the future these can be considered as commercial of the self – COTS) that need to be integrated in order to provide a new service. However, the examples are not exhaustive, as each one of the proposed scenarios can be extended by changing the message flow among the main components or the level of dependability on the IM channel.

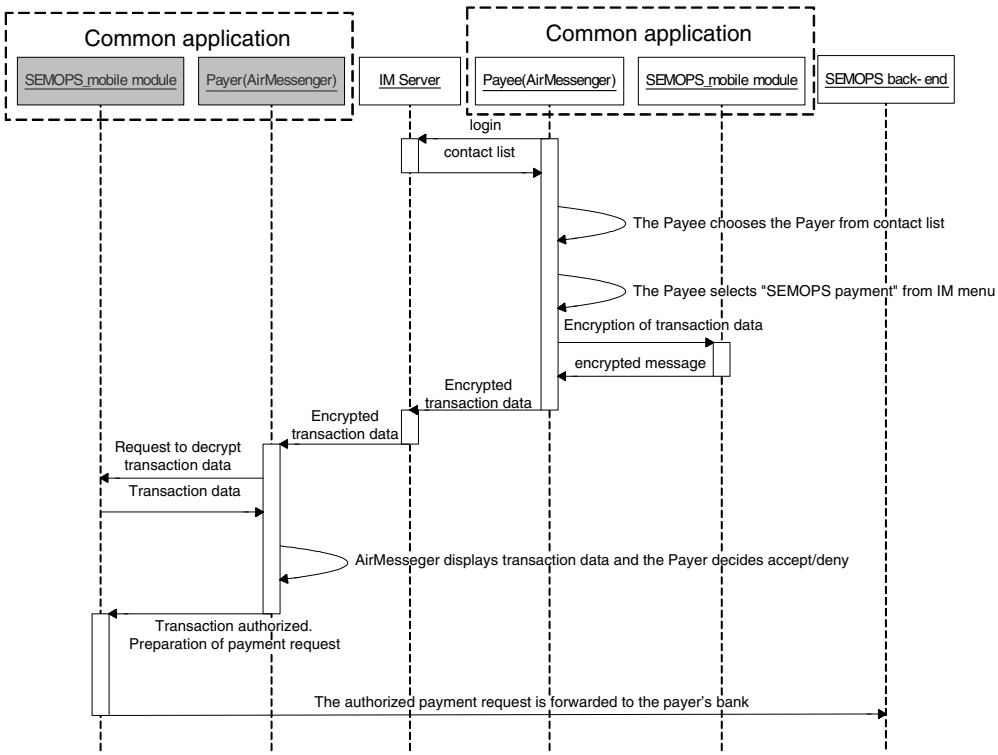

Figure 12.7 Integrated module approach (IM front-end).

12.4.1 Server-based Approach

Figure 12.4 depicts a server-based IMMP. This approach generally assumes that the core service runs on a server and the interactions are proxied via a thin client such as an application on the mobile device. In such a framework the payee interacts with the AirBOT, which is the presence/messaging handling application located on the fixed line. The AirBOT provides the main SEMOPS module functionality, which is then proxied to the mobile device and presented to the user via the AirMessenger. The AirBOT is assumed to integrate the IM server. The payee initiates the payment by providing the IM user ID (which is unique) and the transaction data, which are then processed internally by the AirBOT, and at the end the user authorization is requested. Once the user authorizes the transaction, the AirBOT sends the payment request to the SEMOPS backend, which is installed in the user's payment processor, e.g. his bank. This approach implements a wallet like server-based approach. The whole payment functionality is wrapped at the server side by the AirBOT, and IM is used to send the transaction data and request the real-time user authorization. This provides several advantages as the core application is always under the control of the service provider who can enhance it with new functionality, without having to update the client side in parallel. This can lead to incremental updates and maintenance of a wide variety of clients at end-devices (which could be tailored to the device's capabilities) without affecting the whole IMMP functionality since the core application and logic is on the server side. However, this approach also implies that some personal sensitive data are stored on the service provider side, something that limits the control that the user has on them. Other security and privacy issues include interaction between the operator's gateway and the server components in the Internet. The approach places a direct trust in the service provider that it will manage all personal data of the user. It could eventually intercept the user's communication with other parties, as the service provider is the middle man in any

communication scenario and builds user profiles with private information. The proposed MP design [17] allows totally anonymous payments to be made, something that comes into conflict with this implementation approach. Furthermore [17], in general, it does not provide a wallet-like server based application as the approach here implies, but rather considers that the payment application is under the control of the user in a device that he trusts, i.e. his mobile phone. This is one possible implementation, however it does not satisfy all privacy/security concerns of the proposed MP approach, therefore we will take a look at some alternative solutions.

12.4.2 'Cooperating Clients' Approach

The engineering design of this approach is powered by the fact that we have two different applications, i.e. one of IM and the other of MP, which may evolve independently. In order to do this, we need to define only the abstract communication model between these two applications that will lead to cooperation between them, while both run on the mobile device of the user. Therefore this approach constitutes a thick client; one with minimal support from the server side, e.g. IM tasks. One of the technical problems that arose is that, since both applications will be running as MIDlets, it is impossible (at least for the moment) to have the two independent modules on the mobile device in a cooperation status, e.g. one controlling the other. Of course, a possible implementation approach would be to make this cooperation with external help from the server-side (as depicted in Figure 12.5), which would bridge the two MIDlets with some server-side support, however this would complicate our approach unnecessarily and possibly decrease overall performance.

This approach does not interfere with the parallel evolvement of the MP and IM modules on the mobile device and is therefore compatible with all possible MP scenarios envisaged. As already mentioned, the communication between the MP module and the IM is not done on the device, but by using the server side, which gets the information from the IM and pushes back to the MP module and vice versa. The server bridges the communication between two applications (IM and MP) on the handset, i.e. we have the payee's AirMessegner application transmitting the data to be given to the payer's MP module. The data are received from the payer's AirMessenger and, with the agreement of the user, are forwarded to the IM server, who then pushes then back to the handset, but now to the MP module, which is listening on a specific port. A PUSH like functionality (if not already supported) can be implemented by constantly polling the IM server. However, this approach requires two applications in mobile terminals and it means that the user (payee or payer) has to launch both applications before initiating a transaction. This is a step that we would like to avoid, as leaving too much responsibility on the user side is not desirable, since if one of the applications is not started the whole payment procedure fails. Therefore, we abandon this scenario (although it is feasible) for a future where multi-threaded applications and inter-MIDlet communication and management become a reality.

12.4.3 Integrated Module Approach

As we have seen in the previous sections, it is possible to have two different applications either cooperating on the mobile device with external help, or the IM module proxying a server based MP module, but it may add complexity or introduce unwanted behavior into our system. Therefore, the next logical step is to try to integrate both applications into one 'common application' that will have the functionality of both modules (the IM and the MP). The approach does not allow independent evolvement of its distinct parts, as the integration is now at source level.

Again, we face two possibilities with regard to the front-end interface via which the user will initiate the mobile payment. Basically we have:

- the MP front-end (realized by SEMOPS) with hidden IM functionality;
- the IM front-end with hidden mobile payment functionality.

Each of them, of course, assures an easier and friendlier usage to their respective users. Therefore existing users of SEMOPS would prefer the first case, while those familiar with the IM would probably prefer the second.

The interaction for the first case is depicted in Figure 12.6. The merchant (payee) starts the MP application on his mobile device and chooses to send the payment transaction data via IM. The payer is selected by simply typing his IM UserID. Subsequently the transaction data are sent to the IM server, who then forwards it to the payer's application via IM. The payer accepts the payment and the authorized payment request is then forwarded to his bank. In this scenario, we use IM only to get the transaction data and forward it to the bank once the payer has authorized the payment. This scenario assumes minimal IM intervention and simply proves that IM can act as an alternative to SMS, Bluetooth, IrDA and alike protocols. Furthermore, the user has very limited interaction with the whole IM process; therefore the learning curve is kept to a minimum. Usability research points out that this would mostly help existing SEMOPS users who are already accustomed to the standard process of payments and who would not like any drastic changes to the whole procedure (such as learning how to interact with an IM system).

The second case would have the IM application as the front-end for realizing mobile payments according to the proposed approach [17]. This interaction is depicted in Figure 12.7. The user is assumed to be accustomed to the IM system and its usage for communication with his 'buddies'. Therefore we want to provide added value by integrating a payment service into what he already uses. It is assumed that the payer and the payee have an initial contact over IM, and one wants to send money to the other. In this case, the payee selects the payer from his contact list (or searches through the AirBOT, which features a system-wide search service). The transaction data (M1 message) is encrypted and sent to the payer via IM. At the payer side, the transaction data is decrypted, and the user authorization is requested. Once the user confirms the payment, the payer's MP module prepares and sends a payment request directly to his payment processor, e.g. his bank.

Both Figures 12.6 and 12.7 show a fraction of the whole spectrum of possible mobile payment processes that the proposed architecture [17] can manage. In addition, the diagrams indicate that the payer always accepts the payment and that the payment request is forwarded to the selected payment processor. Of course, in case of a failure, e.g. if the payer rejects the payment, the appropriate notifications are distributed to all parties according to the MP specifications. Both scenarios can be further extended so that the IM is also used among the payment processors as well as the DataCenter. However, in our initial prototype we have focused only on the user mobile front-end scenarios.

12.5 Implementation

A prototype has been developed, implementing the 'integrated module' approach with the IM application as a front-end, proving that the concept is viable. Figure 12.8 shows various screenshots of the Graphical User Interface (GUI). As can be seen, the payee selects IM in his mobile device and logs into the IM server. Subsequently he selects the payer from his contact list and chooses the menu allowing him to fill in the payment info (which will create an M1 message containing the transaction data). After the payer receives the transaction data and accepts the payment, the integrated module forwards the information to the payment processor to realize the actual transaction.

Figure 12.9 shows the internal sequence realized by the integrated IMMP module. The iExternalApp interface allows access to the internal SEMOPS methods from external application. This scenario focuses on handling payments among friends (names existing in the IM 'buddies' list) but not among strangers. However it is desirable that the user can also send messages to persons not existing in his predefined 'buddies' list but also on the fly communicate with new users or be able to search for them in a user database (DB). The latter would enable the user to make payments to total strangers without having to add them to his contact list. This could be typical for one-time transaction scenarios, e.g. when a taxi driver wants to send a payment request to his one time customer. In order to handle this, he either

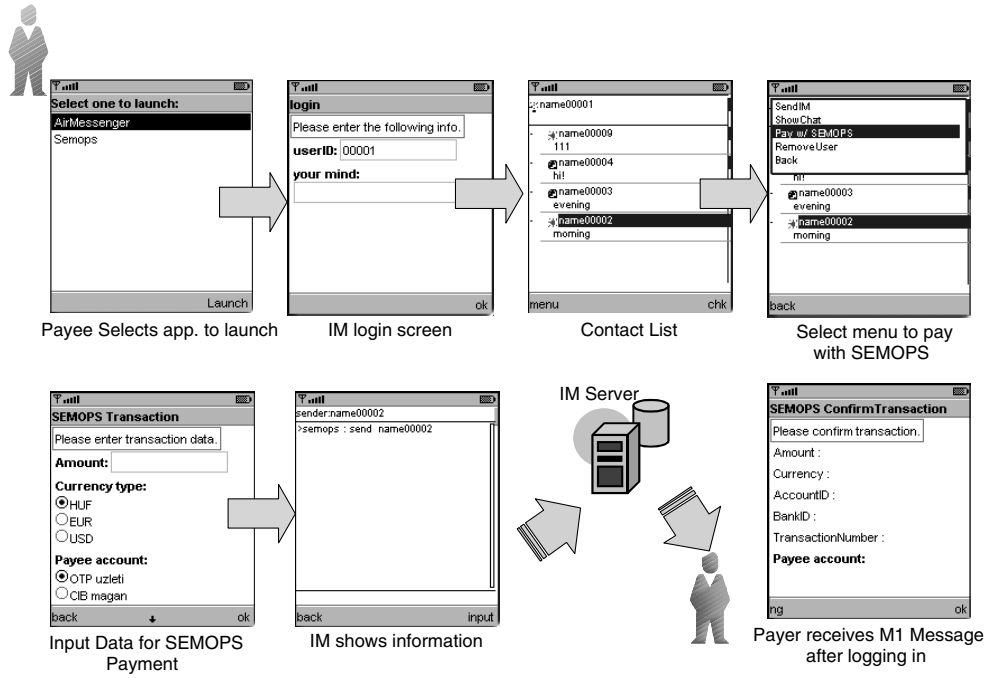

Figure 12.8 IMMP transaction realization.

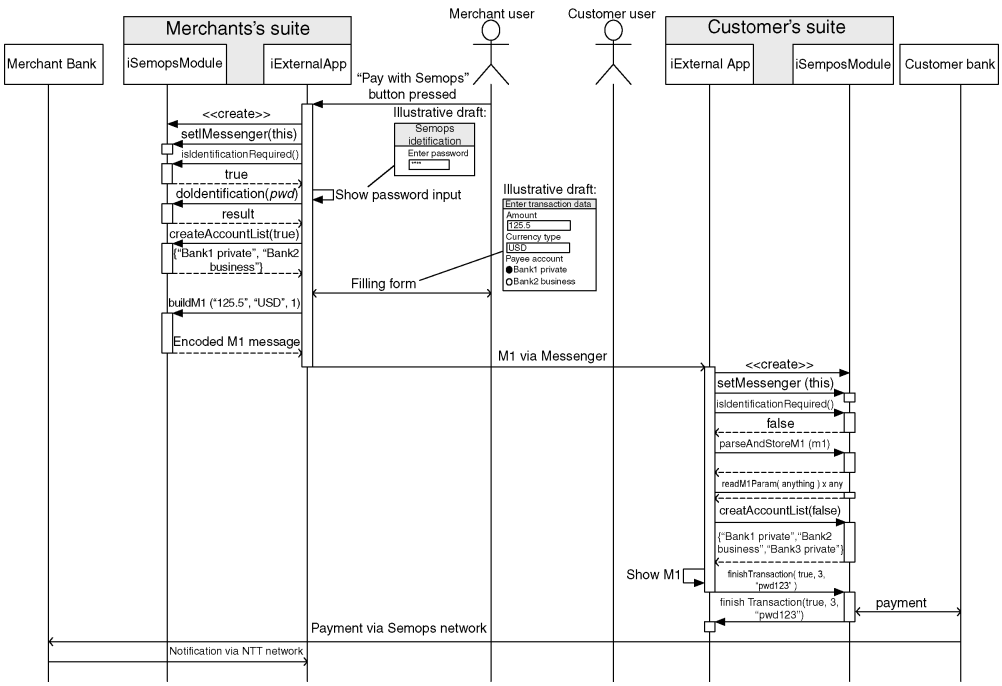

Figure 12.9 IMMP sequence diagram.

has to type the client's IM ID or search for it. Therefore, we developed an additional search functionality (like a white page directory) using the AirBOT. This implies a text-based search with given parameters. The AirBOT can locate a user's IM ID based on several criteria, e.g. search only online users. In the future and in order to protect the user privacy this will be more user controlled (e.g. the user will specify if such a search functionality should list him, and how many of his profile properties should be available to other parties), and even presence features may be added (e.g. the taxi driver is allowed to search only for users within 10 meters of his current location).

Figure 12.10 shows the user interface of our prototype implementation with the search feature as described above. The user only has to choose 'Search User' from his menu or just select the AirBOT which is displayed as a user on his contact list. He can interact with the AirBOT simply by choosing or typing in keywords for the temporary user. These keywords could be associated with a user name, an alias, his mobile phone number, his online or offline status, his current location or other criteria.

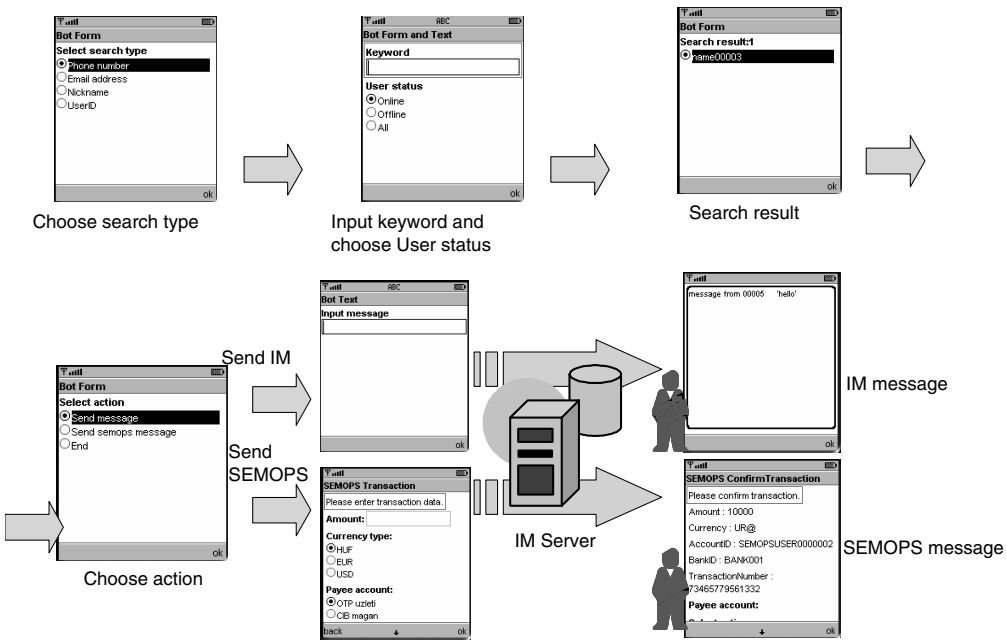

Figure 12.10 IMMP interactive searching functionality.

With regard to the technology side, the implementation was done in Java and is based on MIDP 1.0 specifications without any vendor-specific APIs. The JAR application is about 100 kbytes, which today limits the choice of mobile devices on which this application can run. However, we do not expect this to be a problem, as the latest generation mobile phones on the market do not have these limitations. The current implementation does not use HTTPS for secure transfer of data; instead, the payment related data are encrypted/decrypted as specified in the SEMOPS specifications. We have here to mention that we have tried to adhere to specific requirements [17] and (i) develop an application mainly targeting limited-capability mobile devices, (ii) use open interfaces in order to address a large number of end-devices, and (iii) provide an easy-to-maintain viable approach.

In the future, we plan to migrate to MIDP2.0 and take advantage of the PUSH-like functionality as well as the HTTPS support for specific communication parts. We are also interested in experimenting with mobile Public Key Infrastructure (mPKI) and attribute certificates in order to support fine-grained user, client and server authentication schemes, as well as policy-based management. Making the

approach more user-friendly, secure, personalized and robust, and including cooperation schemes among different IM servers in various administrative domains to enhance the search functionality also provides future challenges.

12.6 Security and Privacy in IMMP

Security and privacy are essential elements for the success of mobile commerce and applications. They are business enablers and not just add-on features. This is because both elements are critical in fostering users' trust towards any mobile services and applications. Security, privacy and trust have been identified as critical enablers for the success of mBusiness by many European Union funded roadmap projects such as PAMPAS (Pioneering Advanced Mobile Privacy and Security [20]) and MB-net (A Network of Excellence on mBusiness Applications & Services [21]) as well as others such as Accenture and CERIAS [22]. IMMP is a combination of a specific MP approach [17] and IM. Because payment procedure is already specified and used by channels complementary to IM in a uniform way, it is clear that integrating IM support must fulfill the security, trust and privacy requirements set by the specifications.

The MP security framework was built with real operational payment processor environments in mind, which put some constraints on the overall approach, as outlined below.

- Banks do not allow encrypted information into the Intranet; therefore, decryption must be done in the Demilitarized Zone (DMZ).
- Banks usually have their own authentication systems, therefore any new MP approach must co-operate with existing infrastructures.
- A global MP approach should be extensible and use heterogeneous channels, including 'strange' ones, like USSD; therefore secure protocols such as SSL/TLS cannot always be used to encrypt the transmission channel.
- Regulations in different countries prohibit the usage of the same keys for encryption and signing; therefore, a new MP approach must have multiple key pairs if encryption and digital signatures are to be used.

Based on these limitations, our MP approach [17] (and therefore also IMMP) gives the security model depicted in Figure 12.11. The termination of the physical channels and the decryption of the messages takes place in the DMZ. The decrypted information reaches the bank module (residing on the Intranet of the bank) through the bank's standard authentication system, which is already used for applications such as home banking. We currently use 1024 bit RSA encrypted XML with 3DES message keys, and 1024 bit 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 12.11.

Strong end-to-end encryption for the transferred data is provided, and different authentication techniques embedded into this encryption can be realized. Purely IM related activities such as logging in an IM server, etc. can be done over secure channels in order to minimize the risk. 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 (at least until the policy/technology framework in the bank changes). The user data that reside on the payment processor are protected with state of the art technology solutions such as encryption, limited availability, key management, etc. The same is true for the data relying on the mobile phone, to which the user has access via an IMMP-specific authentication, such as entering a password. Furthermore, all MP interactions that contain user private data are exchanged securely with a single user-trusted entity, namely his financial service provider. The IDs used in the MP approach masquerade the specific transaction, which is untraceable from only that known information. Since the

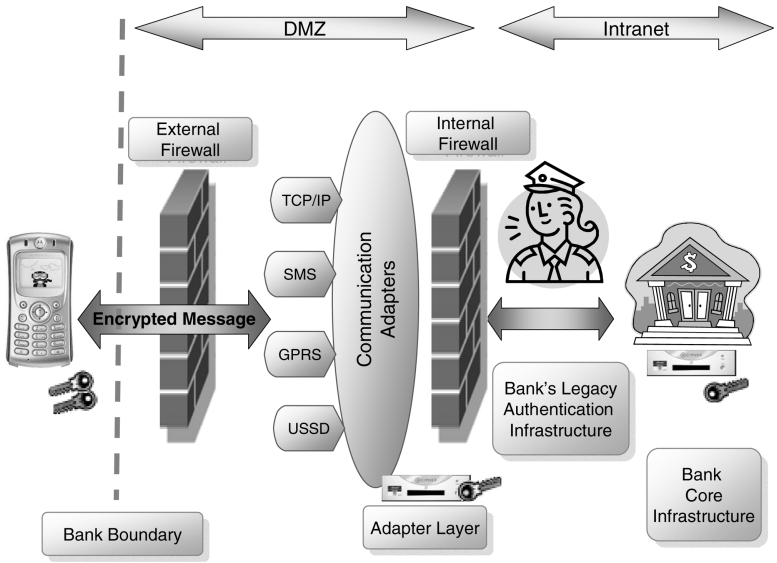

Figure 12.11 Split security operations at payment processor's side.

business model of our MP approach [16] also tackles the privacy, there is no immediate need at the moment to address it further via add-on solutions such as anonymity/pseudonymity services, etc. Add-on services, such as the 'search' function that we introduced, are at the moment in the hands of the service provider. However in the future it is expected that the mobile user will be able to selectively control not only who can access his presence information and when they can access it but also what portion of it would be available for a specific task. This user-controlled privacy coupled with the capabilities of out MP model can make anonymous payment possible, and provide a real alternative to today's cash dominated market.

In the future the IMMP will follow a more sophisticated approach. MobilePKI, mobile digital signatures, encryption, and biometric authentication are expected to be widely available in the future mobile devices (for instance Fujitsu's F900iC 3G handset features a fingerprint scanner). Therefore, it needs to be examined how these methods can be integrated in the system for providing strong security and privacy whenever it is required, and always balancing other requirements such as usability and performance. Furthermore, Identity Management efforts are ongoing for the Internet community and several standardization consortia such as Radicchio (www.radicchio.org) and Liberty Alliance (www.projectliberty.org) are working towards federated identity in the virtual world. If such efforts are successful, they will have a catalytic effect on MP domain, as they will provide a homogeneous identity framework capable of universally bridging the real and virtual worlds. Therefore, efforts, like the newly announced (March 2004) cooperation of NAC, OMA, OSE, PayCircle, SIMalliance and WLAN Smart Card consortium with the Liberty Alliance to demonstrate that federated identity is, among others, a key enabler in mobile payments are steps in this direction. Once this is available it will quickly be integrated to IMMP-like solutions.

12.7 Conclusions

Mobile payments are expected to be of critical importance for the e-/m-commerce domain within the next few years. It is expected that there will be different business models and different technology approaches in the quest for a successful service launch that will reach a critical mass and establish itself

as a global payment service. Within this context we believe that IM coupled with context awareness can be successfully combined with mobile payments. In order to prove this, we designed and implemented such an IMMP service based on a global MP service [17] and an IM platform [14]. Instant messaging is a very interesting approach to realize almost real-time message exchange between the parties in a mobile payment scenario. We have presented the basic technologies that were used, as well as the design dilemmas that arose while trying to realize such a system. We have commented on the pros and cons of the different scenarios and finally implemented one of these as a proof of concept. The prototype described in this chapter has been successfully demonstrated by NTT DATA and the SEMOPS consortium to the general public at the premier information technology event CeBIT 2004 [23].

The authors believe that IM is a promising approach and, once it is extended with presence management capabilities, it can be used as a generic service in future mobile services such as mobile gaming, mobile digital rights management (mDRM) scenarios, etc. The IMMP approach depends on IM and therefore faces the same problems as do IM systems. In future IMMP users may use different IM systems, which brings to the surface the interoperability problem as well as the scalability one for services such as 'search' which we generically introduced. However, there is ongoing work [24] towards developing standardized IM applications, and new approaches [25] that may arise can be easily integrated. Mobile payments and especially person-to-person payments are the most interesting ones, without of course neglecting the IM interaction with a virtual POS. Almost in all the current scenarios of IM, the end-user is assumed to be a human entity or a machine that interacts via a pre-defined process. However, in the future such interaction could be at a more flexible level with the introduction of intelligent agents or expert systems that slip into the customer/merchant roles. Finally, wireless/mobile instant messaging may do for the 2.5 G and beyond infrastructures what e-mail did for the Internet, i.e. open a new technology to the masses. Finally it may become the de facto standard for 3G content services and other applications that may require a real-time presence-enabled framework. Mobile payments within that vision are seen as one successful IM-powered financial service, standalone or as part of more sophisticated applications.

References

[1] Stamatis Karnouskos, Mobile payment: a journey through existing procedures and standardization initiatives, *IEEE Communications Surveys and Tutorials, Vol. 6, No. 4, 4th* Quarter 2004.

[2] Norman Sadeh, *M Commerce: Technologies, Services, and Business Models*, John Wiley & Sons, 2002.

[3] J. Henkel, Mobile payment: the German and European perspective. In *Mobile Commerce*, Gabler Publishing, Wiesbaden, Germany, 2001, http://www.inno-tec.de/forschung/henkel/M-Payment%20Henkel%20e.pdf

[4] David McKitterick and Jim Dowling, State of the Art Review of Mobile Payment Technology, Department of Computer Science Trinity College Dublin, Technical Report, http://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf

[5] EU Blueprint on Mobile Payments, Accelerating the Deployment of Mobile Payments throughout the Union, Working Document, Version 1.1 (draft) – 12-July-2003.

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

[7] Durlacher Research, UMTS Report – an Investment Perspective, London, Bonn, 2001, http://www.dad.be/library/pdf/durlacher3.pdf

[8] SIP for instant messaging and Presence Leveraging Extensions (simple), http://www.ietf.org/html.charters/simple-charter.html

[9] Extensible Messaging and Presence Protocol (XMPP) of the Internet Engineering Task Force (IETF), http://www.ietf.org/html.charters/xmpp-charter.html

[10] Instant messaging and Presence Protocol (IMPP) of the Internet Engineering Task Force (IETF), www.imppwg.org

[11] *The Book of Visions 2001 – Visions of the Wireless World*, Wireless World Research Forum, version 1.0, http://www.wireless-world-research.org, 2001.

[12] Open Mobile Alliance, Wireless Village Initiative, http://www.openmobilealliance.org/WirelessVillage

[13] Secure Mobile Payment Service (SEMOPS), www.semops.com
[14] I. Tanaka, T. Arimura and S. Yokohama, Wireless Instant Messenger Development in the Japanese Market, *Second International Conference on Mobile Business*, 23–24 June 2003, Vienna, Austria. www.mbusiness2003.org
[15] A. Vilmos and S. Karnouskos, SEMOPS: Design of a new Payment Service, International Workshop on Mobile Commerce Technologies and Applications (MCTA 2003). In *Proceedings 14th International Conference (DEXA 2003)*, IEEE Computer Society Press, September 1–5 2003, Prague, Czech Republic pp. 865–869.
[16] S. Karnouskos, A. Vilmos, P. Hoepner, A. Ramfos and N. Venetakis, Secure Mobile Payment – Architecture and Business Model of SEMOPS, EURESCOM summit 2003, Evolution of Broadband Service, Satisfying User and Market Needs, 29 September – 1 October 2003, Heidelberg, Germany.
[17] S. Karnouskos, A. Vilmos, A. Ramfos, B. Csik and P. Hoepner, SeMoPS: a global secure mobile payment service. In Wen-Chen Hu, Chung-Wei Lee and Weidong Kou (eds), *Advances in Security and Payment Methods for Mobile Commerce*, IDEA Group Inc., Nov. 2004.
[18] The Java Message Service (JMS), http://java.sun.com/products/jms
[19] Presence & Availability Management (PAM) Working Group, http://www.parlay.org/about/pam
[20] Deliverable D04: Final Roadmap (Extended Version), Pioneering Advanced Mobile Privacy and Security (PAMPAS – www.pampas-eu.org).
[21] G. Giaglis, P. Ingerfeld, S. Karnouskos, P. Lee, A. Pitsillides, N. Robinson, M. Stylianou and L. Valeri, mBusiness Applications and Services Research Challenges, White Paper, 24th November 2003, MB-net Project (IST-2001-39164).
[22] Roadmap to a Safer Wireless World, Security Report, Accenture and CERIAS, Oct 2002. http://www.cerias.purdue.edu/news_and_events/events/securitytrends/
[23] CeBIT – Center for Office and Information Technology, http://www.cebit.de
[24] Michael McClea, David C. Yen and Albert Huang, An analytical study towards the development of a standardized IM application, *Computer Standards and Interfaces Journal*, **26**(4), 343–355, August 2004.
[25] A. C. M. Fong, S. C. Hui and C. T. Lau, Towards an open protocol for secure online presence notification, *Computer Standards and Interfaces Journal*, **23**(4), 311–324, September 2001.