Universal Approach to Mobile Payments

Stamatis Karnouskos [1], András Vilmos [2]

[1] Fraunhofer Institute FOKUS (www.fokus.fraunhofer.de)
Kaiserin Augusta Allee 31, D-10589, Berlin, Germany
Phone: +49-30-34637172, Fax: +49-30-34638000
email: Stamatis.Karnouskos@fokus.fraunhofer.de

[2] 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

Universal Approach to Mobile Payments

INTRODUCTION

An old saying coming from the telecom world states that nothing can be really considered as a service, unless you are able to charge for it. The last years we have seen a boom in interest in mobile commerce mainly due to the high penetration rates of mobile phones. Furthermore there is evident the need for a real-time, open and trusted payment service, that can be used any time, anywhere and can handle any transaction in any currency. Such a service would promote not only content creating activities but would empower the electronic and mobile commerce area and kick-start new innovative services. The time is right for such a mobile payment service, since the infrastructure, the business models, and other conditions that favor its existence are realistic and in place (Vilmos & Karnouskos 2004). Up to now, we have witnessed the rise and fall of several efforts in the area, ranging from realizing simple intangible good purchases, up to interaction with real points of sale (POS) and person-to-person (P2P) transactions. Day by day, new trials are initiated targeting different sections in the MP area; however there is still no solution that is open and widely accepted. In this article we firstly introduce the reader to the mobile payment area, present the guiding forces behind it and subsequently examine such an open, secure mobile payment approach that has been successfully designed, implemented and tested. Furthermore we identify some mid-term future trends that we consider will be of high importance to the further development of the area.

BACKGROUND

Payments are the locomotive behind the business domain and heavily depend on trust and security. A global study by (Little, 2004) estimates that m-payment transaction revenues will increase from $3.2 billion in 2003, to $11.7 billion in 2005 and $37.1 billion in 2008 world-wide. Mobile payments are seen as the natural evolution of existing e-payment schemes that will complement them (Heng, 2004). 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 motivation reasons for using mobile devices for payments.

The context of mobile payments can be defined as follows: Any payment where a mobile device is used in order to initiate, activate and/or confirm this payment can be considered as a mobile payment. 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 authorizes the transaction to the payment processor for the 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.

Based on the amount to be paid we can have different categorization of mobile payments. Generally we have:

- *Micro-payments:* These are the lowest values, typically under $2. Micro-payments are expected to boost mobile commerce as well as pay-per-view/click charging schemas.
- *Mini-Payments:* These are payments between $2 and $20. This targets the purchase of everyday's small things.
- *Macro-payments:* These payments are typically over $20.

Currently there are several efforts at international level in order to accelerate and solidly support emerging mobile payment solutions. Most of the heavyweight companies that deal with hardware or software products for the mobile market, as well as others such as the mobile network operators (MNO) and financial service providers try via international fora and consortia to define the guidelines such a system should comply to. The aim is to produce an approach that is widely acceptable and that it would reach a global audience and not address just a specific customer base or isolated scenarios. Towards this end several consortia have aroused such as Simpay (www.simpay.com), Starmap Mobile Alliance, Mobey Forum (www.mobeyforum.org), Mobile Payment Forum (www.mobilepaymentforum.org), Mobile Payment Association (mpa.ami.cz), Paycircle (www.paycircle.org), Mobile electronic Transactions (www.mobiletransaction.org) etc. Apart from these "pure" mobile payment consortia whose work directly affects the mobile payments, there are also other actors that indirectly are evolved with the mobile payment area, and come from the financial/banking sector. Karnouskos (2004) provides an overview of these consortia.

For mobile payments to succeed several requirements need to be addressed. Simplicity and usability largely determines whether users will use a service. This includes not only a user-friendly interface, but also, the whole range of goods and services one can purchase, the geographical availability of the service and the level of risk the user is taking while using it. A promising mobile payment service should be offered widely and in a transparent fashion covering the biggest range of mobile payment transactions such as person to person (P2P), business-to-consumer (B2C) and business to business (B2B), domestic, regional and global coverage, low and high value payments. It should be based on open standards that will allow it to interact with other systems and easily scale. It should also be secure by means of technology and processes, and preferably be built on existing trust relationships. The new systems should be at the end, more cost effective than the legacy approaches, e.g. the technology used may cost more but if the fraud is minimized, at the end of the day it is a cost saving solution. Furthermore they should also create new revenue flows or better tackle existing ones in order to justify their existence. Finally understanding the nature and key rules of each local market as well as providing integration with existing approaches (e.g. reuse existing infrastructure and legacy billing systems) may also lead to its rapid acceptance. It should also be kept in mind, that apart from the technology part, the right legislation framework must be in place and ease approaches, especially when we refer to a global payment service. Experience has shown that even when a common directive exists (for instance within the European Union), its full interoperable implementation at per country level still remains a challenging task (Merry, 2004).

Within the past years, several mobile payment solutions have been developed. Some of them even managed to leave the prototype level and enter the commercial market. A detailed insight on these payment approaches is provided by Henkel (2001), Krueger (2001) and Karnouskos (2004). As it has been pointed out, the mobile payment area is an active one and is rapidly changing. However still existing approaches have done little to fully address all of the requirements needed to establish a global, widely accepted open and secure mobile payment service. For instance regarding security in such services; most MP procedures today use SMS or IVR (Interactive Voice Response) as a method to verify user’s identity, methods that have been proven to be insecure. Furthermore, users are usually asked to provide their personal information to a third party service provider in order for them to be able to register and get the service. Therefore they are asked to place immediate trust of their money and personal data on a previously unknown party. This third party is able to have the complete set of data for any transactions users make, therefore it is able to monitor users' private lives and of course do indirect profiling. It must be kept in mind that user-perceived security (the combination of technical security and trust in the procedures of the approach) is a critical factor (Heng, 2004) that decides on the success or failure of a payment service and therefore it has to be done correctly from day one. Generally existing solutions today are either not trusted, not available to a large enough audience, not speedy enough, not user friendly, not secure enough, tailored for special applications and transaction types, are only available to a limited closed circle of customers and merchants, or have a limited business model. SEMOPS, which we shortly present here, has designed and implemented an approach that realizes a secure, universal, real-time electronic payment service, which effectively covers most of the requirements such a global service poses. To our knowledge past and current mobile payment approaches (Karnouskos, 2004), address only fractions of the mobile payment domain needs, while SEMOPS takes a holistic approach, therefore complementing any existing system.

SEMOPS: A SECURE MOBILE PAYMENT SERVICE

SEMOPS is a mobile payment solution that is capable of supporting micro, mini as well as macro payment 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 person to person (P2P), business to consumer (B2C), business to business (B2B) and of course person to machine (P2M), with a domestic and/or international geographic coverage.

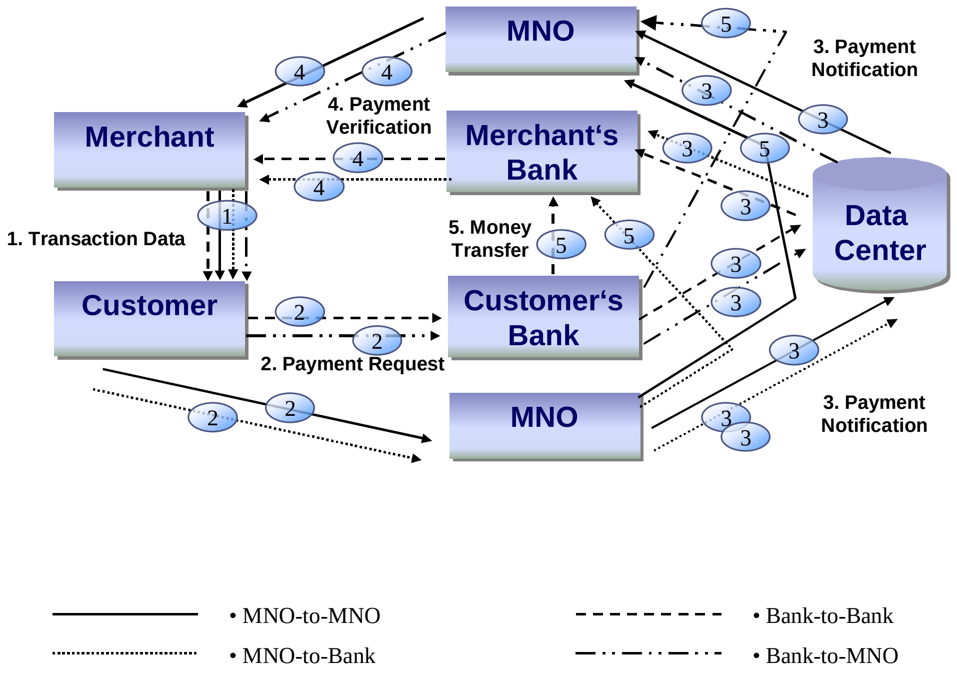

Figure 1 - SEMOPS transaction flow

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 realized 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. The payment service designed, developed and currently in trial within the SEMOPS project establishes a transaction flow, which is customer-driven and follows a simple credit push model. Basic principle of the business model is that it is based on the cooperation of banks and MNOs. This situation has two consequences a) actors’ resources can be combined and b) revenue has to be shared. This is quite a challenge but SEMOPS proves that this is a win-win situation for all participants.

In Figure 1, one can distinguish the main players and components in a mobile payment scenario. Each user (customer or merchant) interacts with his/her payment processor e.g. home bank or mobile network operator (MNO) only. The banks and MNOs 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 SEMOPS infrastructure and are used as usual. A typical scenario assumes that:

1. The merchant (generally any real/virtual POS) provides to the customer the necessary transaction details, invoices.
2. The customer receives the transaction data and subsequently initiates the payment request, authorizes it and forwards it to the payment processor (at the customer’s bank or MNO).
3. The payment processor identifies the customer, verifies the legitimacy of the payment request, checks the availability of funds and forwards this request to the merchant’s payment processor via the DataCenter (DC).
4. The merchant’s bank receives the payment notice, identifies the merchant, notifies him/her about the payment being made, or requests from him to confirm or reject the transaction.
5. Once the merchant side confirmation comes, the fund transfer is done and all parties are notified about the successful payment.

There can be different combinations, depending on whether the user (customer or merchant) uses his/her bank or MNO account and whether the merchant accepts the payment in his bank or MNO account. The SEMOPS model (Karnouskos, Vilmos, Hoepner, Ramfos, Venetakis, 2003) is extensible, therefore any third service provider that can offer the customer an account (e.g. credit card or financial service provider, even a utility company) can also easily slip in the role of the bank. It is however important to note, that although SEMOPS enables any account managers to play the role of a payment processor, the actual participation may be limited by legal constrains.

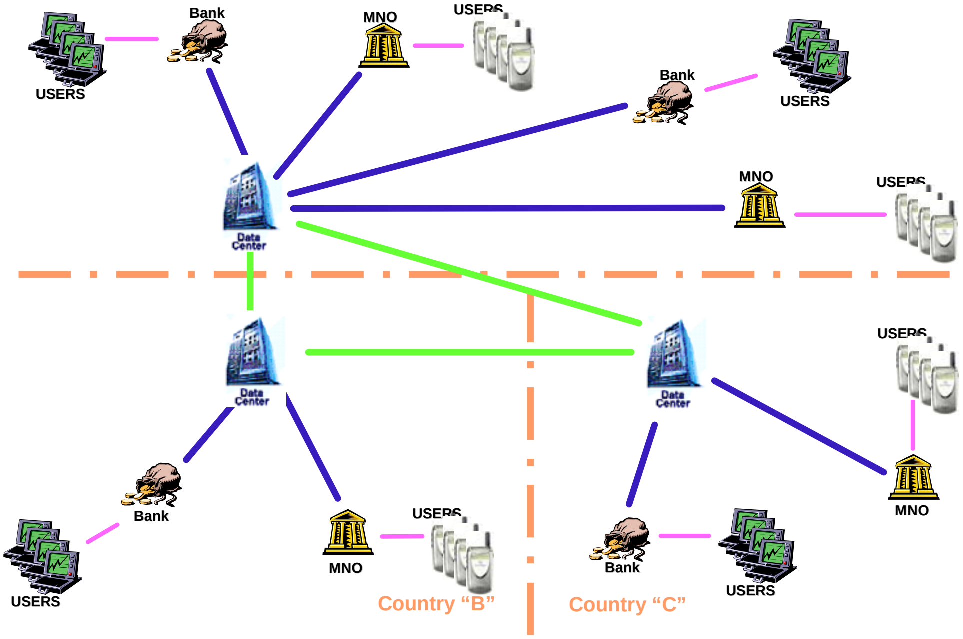

Figure 2 - Distributed MP service architecture

The new payment solution only has a chance to be accepted on the market if it makes good economic sense for the key players to promote the service. All the features, offered to the end users, the security, the comfort, the wide reach may be in vain if there is no economic incentives for the service providers. However it is obvious also that the service providers alone cannot make a success story of the service if the users are dissatisfied with either the service or the terms of the usage. The SEMOPS approach is based on decentralization. In each country where the service is introduced there is a local entity, the license holder, who organizes the service, contracts with the banks and mobile operators, contracts with the local service providers, ensures that local regulations are complied with, makes sure that the general service requirements are followed.

The flexibility of the model and its capability of integrating quickly new payment processors is critical for its survival. As it can be seen in Figure 2, the customers of any new financial provider that connects to the infrastructure can immediately transact with all other customers of the other providers in a transparent for them way. That will lead to a rapid expansion of the service that can establish it as a global payment service. SEMOPS follows a trust-delegation model. The new customers added do not have to place any trust into the SEMOPS approach itself; they need to trust the service that their banks and MNOs are providing to them (therefore extend the existing trust they already have placed to these institutions). The banks and MNOs are connected via a financial infrastructure with its own rating system and its own trust relationships that exist today. As a result, in a transaction scenario, user A does not have to know personally or trust directly user B to perform the transaction. The SEMOPS approach has several features, including means to secure transactions, notify in real-time its users and protect their privacy by even allowing anonymous payments to be made. Further info on the approach can be found in (Karnouskos, Vilmos, Ramfos, Csik, Hoepner, 2004). Beyond using existing trust relationships among banks/MNOs and their customers, SEMOPS deploys also state of the art security (digital signatures and encryption) as well as processes that protect the user privacy (Karnouskos, Hondroudaki, Vilmos, Csik, 2004).

FUTURE TRENDS

Currently almost all existing approaches focus on 2G or 2.75G infrastructures in order to achieve the critical mass once they are commercial. However, the mobile network infrastructure itself is rapidly evolving. The début of UMTS, wireless LAN, WiMAX and other 3G and beyond technologies will provide new capabilities that will free MP from some its current limitations and allow more sophisticated approaches to be developed. Once this infrastructure becomes mainstream, we will witness also solutions that take into account the new non-existent today security capabilities offered by such infrastructure for security, privacy and trust management.

The device manufacturers continue to bring on the market mobile phones that have advanced capabilities and host their own execution environment. It is a matter of time until advanced cryptographic services are integrated in these devices, that will make possible diverse secure communication and authentication procedures. Mobile public key infrastructure (mPKI), mobile digital signatures, encryption, and biometric authentication are expected to be widely available in the near future. 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) work towards federated identity in 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 bridging universally the real and virtual world.

With the rise of technological approaches, other communication channels will flourish. Today the basic channels of payment services are the SMS, Voice, and lately IrDA and communication over GPRS/EDGE. However other innovative approaches seem also promising such as Instant Messaging (IM) and Near Field Communications (NFC). The IM will not only allow bridging together the Internet and mobile services and payments, but will also make trivial

P2P payments where the two or more parties are not in the same physical space (Karnouskos, Arimura, Yokoyama, Csik, 2005).

Digital Rights Management (DRM) is an integrated complex context covering not only technologies that limit or prohibit the unauthorized copying or distribution of these products but include also laws, contracts and licenses that regulate and restrict the use of such material (Becker et al., 2003). As content generated for mobile devices is increasing, mobile DRM systems are expected to play a significant role in the future (Beute, 2005). Standardization initiatives like the Open Mobile Alliance (OMA - www.openmobilealliance.org) work towards developing an advanced mobile DRM standard with the ability to support richer content business models. However rich payment capabilities also need to be in place and the existing MNO billing schemes will not be enough. In the future coupling content management with a global payment capability, preferably real-time e.g. via Instant Messaging, will result in a powerful combination, where the mobile user any time anywhere can access legitimately content and instantly pay for it according to his preferences (Karnouskos, 2004).

CONCLUSION

Mobile payment has sparked a lot of interest in research and commerce communities and is viewed as an integral part of our future life. The area is an extremely active one, and rapid commercial evolvement is expected in the short and mid term. The need for a mobile payment service that can address in a global way existing needs is evident, and the first steps have already been done. However, although several mobile payment services have been designed, implemented and even commercialized, up to today there is no such service that can be widely accepted and cover adequately most of the transaction spectrum that we have referred to. For any service to evolve and reach the critical mass, several issues including business as well as technology aspects have to be approached in the right way.

SEMOPS (www.semops.com) presents a promising approach as it integrates state of the art technology, a flexible cooperative business model and builds over trust relationships that exist in the real-world today. SEMOPS demonstrated a fully functional service with live users in the premier computer industry event CEBIT 2005 (www.cebit.de). Currently we are in the process of setting several pilots mainly in Europe, but later also in Asia and U.S.A., while the aim is to make SEMOPS a successful commercial service within the short-term future.

REFERENCES

Becker, E., Buhse, W., Günnewig, D., Rump, N. (editors), (2003). “Digital Rights Management Technological, Economic, Legal and Political Aspects”, Lecture Notes in Computer Science, Vol. 2770, (ISBN: 3-540-40465-1).

Beute, B. (2005), Mobile DRM—usability out the door?. Telematics and Informatics, Elsevier , pp. 83–96.

Heng, S. (2004). E-Payments: modern complement to traditional payment systems. Economics: Digital Economy and structural change, Deutsche Bank Report, May 6, 2004, No 44, Deutsche Bank Research.

Henkel, J. (2001). Mobile Payment: The German and European Perspective. G. Silberer (ed.): Mobile Commerce, Gabler Publishing, Wiesbaden, 2001.

Karnouskos, S. (2004). Mobile Payment: A journey through existing procedures and standardization initiatives. IEEE Communications Surveys & Tutorials, Vol. 6, No. 4, 4th

Quarter 2004. URL: http://www.comsoc.org/livepubs/surveys/public/2004/oct/pdf/KARNOUSKOS.pdf

Karnouskos, S., Arimura, T., Yokoyama, S., Csik, B. (2005). Instant Messaging enabled Mobile Payments. In the book of Apostolis Salkintzis, and Nikos Passas (editors), “Wireless Multimedia: Technologies and Applications”, published by John Wiley and Sons Ltd, Aug 2005.

Karnouskos, S., Hondroudaki, A., Vilmos, A., Csik, B. (2004). Security, Trust and Privacy in the SEcure MObile Payment Service, 3rd International Conference on Mobile Business 2004 (m>Business), 12-13 July 2004, New York City, U.S.A.

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.

Karnouskos, S., Vilmos, A., Ramfos, A., Csik, B., Hoepner, P. (2004). SeMoPS: A Global Secure Mobile Payment Service. In the book of Wen-Chen Hu, Chung-Wei Lee, and Weidong Kou (editors), “Advances in Security and Payment Methods for Mobile Commerce”, IDEA Group Inc., Nov 2004 (ISBN 1591403456).

Krueger, M. (2001). The future of m-payments – Business options and policy issues”, Electronic Payment Systems Observatory (ePSO), Institute for Prospective Technological Studies, August 2001.

Little, A. (2004). Global M-Payment Report 2004 – Making M-Payments a Reality. Report published by the strategy consultancy Arthur D. Little, July 2004, www.adlittle.com

Merry, P. (2004). Mobile Transactions in Europe: The Challenge of Implementation and Ramifications of EU Directives. Industry Survey from the ARC Group, July 2004, www.arcgroup.com

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

Vilmos, A. & Karnouskos, S., (2004). Towards a Global Mobile Payment Service. 3rd International Conference on Mobile Business 2004 (m>Business), 12-13 July 2004, New York City, U.S.A.

TERMS

- **Mobile Payment:** Any payment where a mobile device is used in order to initiate, activate and/or confirm this payment can be considered as a mobile payment.
- **Micro-payment:** These are the lowest values, typically under $2. Micro-payments are expected to boost mobile commerce as well as pay-per-view/click charging schemas
- **Mini Payment:** These are payments between $2 and $20. This targets the purchase of everyday's small things.
- **Macro-payment:** These payments are typically over $20.
- **Authorization:** Granting of rights, what includes granting of access based on access rights or privileges. It implies the rights to perform some operation, and that those rights or privileges have been granted to some process, entity, or human agent.
- **POS:** Point of Sale is a location where a transaction occurs. This may be a realPOS e.g. a checkout counter, or a virtualPOS e.g. an e-shop in the Internet.

- **DRM:** Digital Rights Management (DRM) is a concept for managing and controlling the access and utilization of digital assets.