Category: Concepts, Trends, and Challenges

Universal Approach to Mobile Payments

Stamatis Karnouskos
Fraunhofer Institute FOKUS, Germany

András Vilmos
SafePay Systems, Ltd., Hungary

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 several years 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 that 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, because 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 first 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 midterm 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) estimated that m-payment transaction revenues would increase from $3.2 billion in 2003, to $11.7 billion in 2005, and to $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 or herself 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:

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

Currently, there are several efforts at the international level 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 and companies such as the mobile network operators (MNO) and financial service providers try via international fora and consortia to define the guidelines

to which such a system should comply. The aim is to produce an approach that is widely acceptable and that would reach a global audience and not address just a specific customer base or isolated scenario. Towards this end, several consortia have aroused such as Simpay (www.simpay.com—ceased operation in summer 2005), 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), and so forth. 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). 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.

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. Typi-