MOBILE FINANCIAL SERVICES: A SCENARIO-DRIVEN REQUIREMENTS ANALYSIS

Kousaridas Apostolos, Parissis George and Apostolopoulos Theodore
Athens University of Economics and Business, Department of Informatics, Patision str 76, Athens, Greece

Keywords: Electronic payments, electronic banking, mobile services.

Abstract: Mobile devices are expected to extend financial information systems, providing additional communication interfaces and new dimensions in computing. Several architectures and commercial systems have been proposed and implemented during the last years for m-payment and m-banking services. However, few of them have met wide acceptance. In this paper, a real case scenario is described; where payment and banking services are taking place using a mobile phone. Through this scenario, we identify the main characteristics and the fundamental functional and technological requirements that should be satisfied by advanced mobile financial systems.

1 INTRODUCTION

One of the most important processes, in the so called electronic society, is the attempt to digitalize economy and financial transactions, by exploiting communication and computing technologies that are continuously evolving. Financial electronic services include banking transactions and payments, which can take place using various means of payment, like credit/debit cards, bank transfers and e-coins. Mobile devices, which may vary from simple cell phones to advanced smart phones as well as PDAs, are becoming commodity. Thus, usage of mobile devices, as payment instruments (Varshney, 2002) or as bank agents (Mallat et al., 2004), has become feasible and will surely facilitate electronic business and more specifically mobile electronic commerce.

During the last years, several payment systems have been proposed and implemented (Karnouskos, 2004). The research community has proposed several architectures and systems, as regards as financial and especially e-payment services, where a mobile device is the instrument for payments' initiation, activation and confirmation. Zhang et al. (Zhang et al., 2004) describe a biometrically enabled mobile payments' solution that uses Java Smart Card technology. Labrou Y. et al. propose a wireless wallet (Labrou et al., 2004) that supports three types of financial transactions: Peer-to-Peer, Web-Store Front and physical Point of Sale (POS). SEMOPS (Ramfos et al., 2004) is regarded as one of the most advanced universal payment system that was developed following the principles of universality, openness and independence from MNOs, banks and technology.

Apart from research initiatives there are several commercial payment systems that have been recently developed, using different payment schemes and various technologies, like voice, WAP and SMS. Mobile FeliCa (Mobile FeliCa, n.d.), Pay Pal (Pay Pal, n.d.), Pay Box (Paybox, n.d.), Nokia Wallet (Nokia Wallet, n.d.) and Vodafone's m-pay bill (Vodafone's m-pay bill, n.d.) are some of the most known commercial solutions.

However, few of them have been widely adopted, due to technological restrictions, hard to use front-ends and absence of substantial motives for involved parties and especially mobile device owners. Development of universal standards, regulation and allocation of roles, among involved entities, are some of the issues that have to be settled for the evolution of m-payment and m-banking systems. The development of more sophisticated mobile devices, the introduction of next generation mobile communication infrastructures and the adoption of Internet technologies create new opportunities for the evolution of financial information systems. The ability to provide and use financial services in a multi-stakeholder environment, taking into account the requirements that banks, merchants and clients have and the

Apostolos K., George P. and Theodore A. (2007).
MOBILE FINANCIAL SERVICES: A SCENARIO-DRIVEN REQUIREMENTS ANALYSIS.
In *Proceedings of the Third International Conference on Web Information Systems and Technologies - Society, e-Business and e-Government / e-Learning*, pages 151-156
DOI: 10.5220/0001282501510156

restrictions that the corresponding actors pose, is investigated in this paper. By analyzing a real case scenario, we try to confront different and sometimes conflicting requirements in order to design a system, which is able to integrate mechanisms and Internet technologies for the effective extension of financial information systems, towards a more mobile environment.

The remainder of the paper is organized as follows. In section 2, we describe a simple running example, which leads us to the identification of some key functional and technological requirements that must be taken into consideration, when designing a system that provides mobile financial services. Furthermore, the requirements and the constraints that were extracted from the scenario analysis are discussed in Section 3, as well as the proposed technologies and standards that must be used, in order to deploy such a system. Finally, the main conclusions, derived from previous sections, are presented in Section 4.

2 SCENARIO ANALYSIS

As Figure 1 depicts, a mobile device can be used to conduct advanced or routine banking services through Internet. It can also be used to issue electronic payments, using various means, for remote or local purchases from physical shops, vending machines or even online shops (Internet point of sales). Furthermore, a mobile device could be the instrument for electronic money transfer among peer mobile devices.

In the sequence, a real-case unified scenario, which incorporates many issues that financial transactions raise, is described. By analyzing this scenario, we try to identify the fundamental functional and technological requirements as well as the prospective technological solutions. Most of the operations, like authentication, authorization and decision support that Alice conducts are taking place through the bank, which is considered as a trusted entity. Bank's decision support system (DSS) is an infrastructure that already exists and only a new interface to the mobile device is exported. On the other hand, operations like physical interaction with the POS and e-coins transfer are conducted directly with the POS or a peer entity. Alice wants to buy a product from an unmanned POS, which is Bluetooth enabled, using her intelligent mobile device.

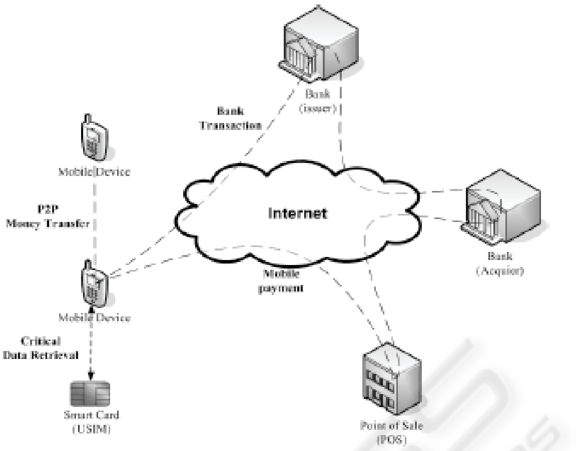

Figure 1: Mobile Payment Context.

She selects the desired product, by physically interacting with the POS, which provides several ways for the payment including e-coins, bank transfers and credit or debit cards. Alice, considering the amount of the transaction, omits bank's decision support system proposal to pay using her credit card, and she selects to pay using her debit card. Afterwards, she is informed that debit card's account is empty, and, thus, it cannot proceed with the payment process. Thereafter, Alice decides to use electronic coins for this micro-payment. Unfortunately, she notices that she has spent all her digital cash and decides to ask her friend Bob to lend her some money. She requests electronic coins from her friend's mobile device, conducting peer to peer money transfer, as happens in our daily transactions, using paper money or coins. After the accomplishment of the P2P transfer, Alice can eventually proceed to pay the vending machine, using electronic coins. Since payment is completed, she receives the product, which she has just bought as well as an electronic receipt.

Further on, our hero chooses to book theater tickets from an Internet box office, by using her mobile phone's browser to fill show's information, and her mobile phone, to expedite the electronic payment. Taking into consideration the payment means that the online shop accepts and the restrictions it may pose, Alice, this time, agrees with the bank's decision support system proposal and decides to charge her credit card. After the accomplishment of the payment, Alice receives the electronic tickets from the online box office. Eventually, Alice requests an analytical report with the transactions that she has conducted during this day and the total charge of the utilized payment means.

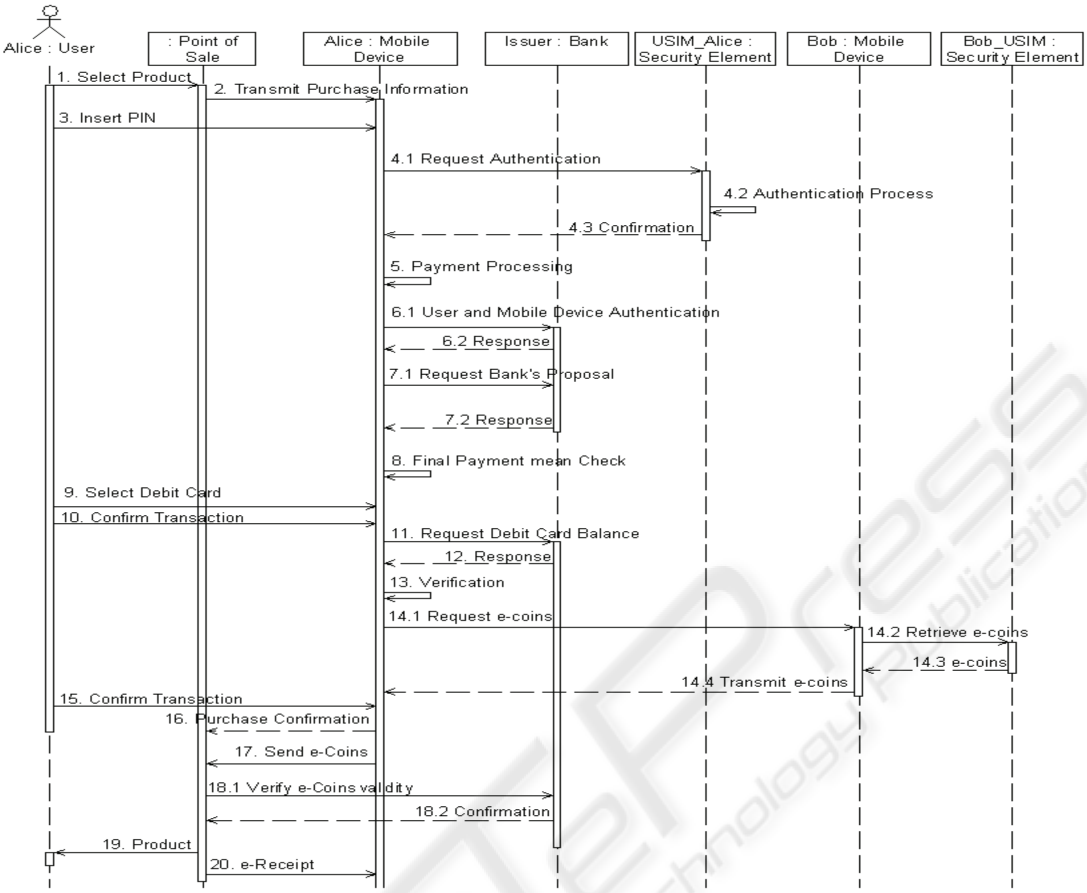

Figure 2: Point of Sale Payment - UML Sequence Diagram.

Figure 2 depicts the interactions among entities and the sequence of messages, which are necessary for the implementation of the first part of the above described scenario. After product's selection (1), the user holds her mobile device near merchant's Bluetooth interface for transaction's initiation. The POS transmits the purchase information to the mobile device (2). This information may include: Transaction's unique code number, Product's information (e.g. Product's Name, Category, Transaction's Timestamp, and Price) and POS's information (e.g. ID, Place, Available payment means).

The device issues a request to the user for authentication in order to proceed with the payment. Alice initiates the payment procedure, by inserting her PIN (3) and the authentication process takes places in the USIM smart card, where critical information is stored (4.1 - 4.3). Upon user's local authentication, transaction's processing is launched (5). Bank's decision support system, after user's and mobile device's authentication (6.1, 6.2), taking into account the available payment means that the online shop supports, the amount of the transaction, user's profile and transactions' history, checks her accounts balance and finally proposes the optimal mean of payment (7.1, 7.2, 8). In the specific case the DSS proposes Alice to use her credit card. However, she prefers to use her debit card (9) and confirms the transaction (10). The local verification subsystem checks the balance of the debit card (11, 12) and informs the user that the debit account is empty, so it is not possible to continue the transaction and proceed to the payment phase (13).

Afterwards, Alice decides to pay using electronic coins, which she will borrow from her friend's peer mobile device. Alice requests electronic coins from Bob's mobile device (14.1). The digital cash is transmitted either over the Internet or using short range wireless technology, if the peer mobile device is nearby. Bob, after authentication and authorization process, retrieves the electronic coins (14.2, 14.3), from his USIM Smart Card, and transmits them to Alice (14.4). Then, she accepts the pending purchase (15) and informs the POS that she will pay, using e-Coins (16).

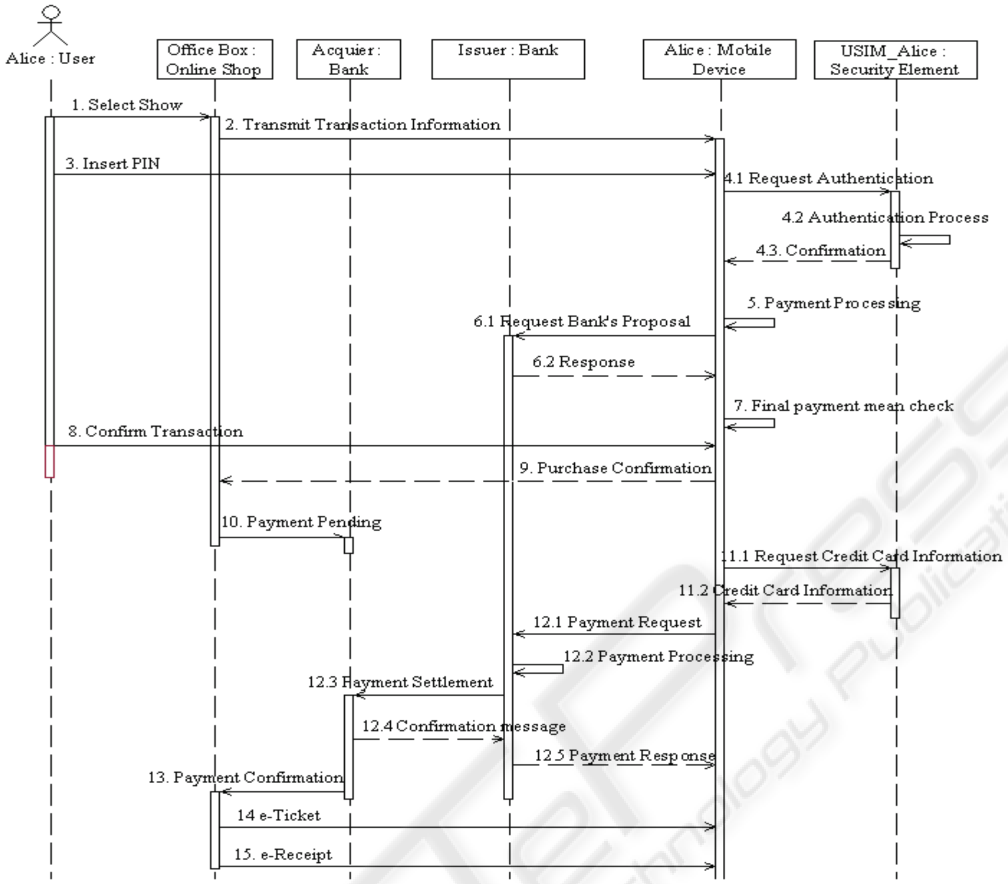

Figure 3: Online Payment - UML Sequence Diagram.

Alice’s mobile phone transmits the e-Coins to the POS (17). The latter can verify their validity from the issuing authority (18.1, 18.2). The recipient and each entity that stores electronic coins can verify digital coins’ authenticity and validity through its issuing bank, preventing the forgery of the digital money. After payment’s settlement, the vending machine delivers the product (19) and sends the electronic receipt to Alice mobile device (20).

Figure 3 illustrates the second part of the scenario, regarding the online payment procedure for the theater’s tickets booking. Alice uses her browser to fill the necessary information regarding the desired show and proceeds to the payment phase (1). The online shop processes her choice and transmits the transaction’s information as well as the available payment means to the mobile device (2). Mobile device’s local payment application undertakes to finalize the payment procedure, through the corresponding payment API, by interacting with the browser. Transactions information that the online shop sends are utilized from the above mentioned payment API, which is responsible for online payments. Alice inserts her PIN (3) in order to authenticate herself locally (4.1, 4.2, 4.3) and the payment process is initiated (5). If the previous established session, with the issuing bank, has expired, user and mobile device’s authentication process is repeated, as described in Figure 2. Alice accepts bank’s proposal (6.1, 6.2) and selects the way she wants to pay, which for the specific case is her credit card (7, 8). The online shop is informed that the user has accepted the purchase (9) and asynchronously informs its acquirer that a payment is pending and that it is expecting a confirmation for the specific transaction (10). Its transaction is identified by a unique code number, which the online shop sends to the mobile device. The application requests and retrieves from the USIM smart card the credit card information (11.1, 11.2) and over UMTS or WiFi communication network, asks from the issuer to credit the account that is associated with the specific credit card (12.1). The issuer processes the request (12.2) and calls the acquirer to settle the pending transaction (12.3). After acquirer’s confirmation (12.4), the issuer informs the mobile device that the transaction has successfully concluded (12.5). The inter-banking system realizes the real transfer of money from the issuer to the acquirer according to their business agreement and not necessarily in real time. The online box office is also informed by the acquirer that it has been paid for the pending transaction (13). Finally, the Internet shop delivers to the mobile device the electronic tickets (14) and the corresponding electronic receipt (15).

The last part of the scenario describes a usual banking transaction, where Alice requests a report for the transactions that she has conducted during this day. She is also informed about the payment means she has used and the respective charging. The direct communication channel allows the information system of the bank organization to offer Alice, personalized services according to her needs and alert messages for unusual operations.

3 SYSTEM REQUIREMENTS

In this section we outline the main technological and functional requirements that are derived from the aforementioned unified scenario and we are trying to identify system properties, which could drive to a complete and sophisticated mobile financial services' system development. First of all, the development of user friendly interfaces at the mobile side, which facilitate browsing and eliminate information insertion and thus, make transactions faster, is an important factor for user acceptance. Smart client model is regarded as the most appropriate way to develop mobile device application, by providing greater autonomy and extension attributes. For instance, Java 2 Micro Edition (J2ME) programming language could be used to implement a smart client model (Java 2 Platform Micro Edition, n.d.).

Platform and language independence is a key requirement, in order to design a universal system. Usage of various programming languages and operating systems, on the involved entities (mobile device, banks and POS), should not affect payment and banking procedures, as described in the scenario. Web services and especially WSDL files are appropriate for definition of communication interfaces, allow language independence and assure the desired platform interoperability and openness. Mobile Web Services (Pilioura et al., 2003) is the technology that could be used for the implementation of such interfaces among mobile device, POS and bank application servers. Web Services model uses Simple Object Access Protocol (SOAP) and Web Services Definition Language (WSDL), for service provision and service description respectively. WSDL files describe how to use software service interfaces and operations that the bank and the POS offer to the mobile device. Furthermore, WSDL files outline the messages, with the corresponding parameters, and data types, which are being exchanged between these entities. Financial services could be invoked over the World Wide Web using SOAP messages, which are XML-based, and could be used for the implementation of communication between involved entities and for exchanging structured information.

Furthermore, security is regarded as one of the most crucial factors for mobile financial systems' adoption by the involved entities (users, banks and merchants). Mobile device's user local authentication is necessary prior to payment or banking process initiation, to ensure that only the owner of the mobile device uses the financial application. The user inserts the corresponding PIN number and her authentication and authorization is taking place at the USIM smart card, which has advanced security mechanisms and is considered as a safe execution environment. Alternatively, biometric mechanisms that provide advanced security could also be exploited. Java Card USIM (Java Card 2.2 Platform Specification, n.d) could be used to store critical information and Java Card applications could be implemented using Java card platform. For the communication between the mobile device and the Smart Card, "Security and Trust Services API" (SATSA) (JSR 177: Security and Trust Services API for J2ME, n.d.) could have been utilized. USIM smart card is a safe place to store e-coins, since, in case a user wants to switch to a new mobile device, she only has to replace the corresponding USIM.

User should also be authenticated to the bank organization, when she wants to conduct a payment through the issuer or to use a bank service. Furthermore, data transmission should be confidential. Each mobile device has communication and cooperation interfaces with bank organizations (issuer), local or remote POS and some other peer mobile devices. Bank organizations must be the central entity in a mobile financial services' system, since it is trusted by users. This fact allows the implementation of advanced security measures. On the other hand, mobile device may transact with several points of sale or peer mobile devices, which regularly change. This makes security issues complex and requires mobile device to avoid interchanging crucial information with these entities, during payment phase, in order to reduce potential threats and establish simple secure connections. The approach to conduct payments through the issuer, utilizing bank's guaranties, ensures that critical information, like credit or debit card numbers, are securely transmitted, since different and safer channels are used. Kerberos system or a Public Key Infrastructure (PKI) could be used for user's authentication and authorization at the side of the bank. In case of peer-to-peer communication or a local payment, the connection with the corresponding peer entity is established through a short range technology like Bluetooth, NFC or Infrared.

Legacy applications integration is an important acceptance factor for financial organizations and merchants. Applications should be developed using an adaptable and upgradeable perspective, taking into consideration the fact that there are various types of mobile devices, which have different radio air interfaces (RATs) or hardware resources, and various POS, which support different communication, payment or security mechanisms. Each financial transaction should be adapted according to the common available technologies that the involved entities support. Mobile device and POS financial applications can be easily upgraded, utilizing over-the-air management and download mechanisms (OMA Download over the Air, n.d.). More sophisticated services must be provided, in order to exploit cooperation between banking and payment modules and introduce intelligence into mobile device, which must not be considered as a simple graphical interface but as a device that takes decisions and makes proposals.

Moreover, the cost for using mobile financial services and the operational cost that is imposed on banks and POS is an issue that should be considered, during system design. Legacy applications integration retains cost low for banks and POS, while offline browsing, which is feasible using smart client model, enables user to use her device without the need to continuously interact with the bank or POS server.

4 CONCLUSIONS

In this paper, we have firstly presented the technological background and the related work in the field of mobile financial services. The technological restrictions and the fact that these systems were designed to satisfy only specific cases have led to limited adoption of mobile payment and banking solutions. A real-case unified scenario was utilized in order to identify the fundamental functional and technological requirements as well as the prospective technological solutions, regarding the design and implementation of such systems. User friendly interfaces at the mobile side, mobile device autonomy, platform and language independence, end to end security, legacy applications integration and low operational costs are some of the derived requirements for a successful mobile financial system development.

REFERENCES

Varshney, U. (2002). Communications: Mobile payments. COMPUTER, 35(12):120–121.

Mallat, N., Rossi, M., and Tuunainen, V. K. (2004). Mobile banking services. Commun. ACM, 47(5):42–46.

Karnouskos, S. (2004). Mobile payment: A journey hrough existing procedures and standardization initiatives. IEEE Communications Surveys and Tutorials, 6(4).

Zhang, Q., Moita, J. N. B., Mayes, K., and Markantonakis, K. (2004). The secure and multiple payment system based on the mobile phone platform. In Workshop on Information Security Applications (WISA).

Labrou, Y., Agre, J., Ji, L., Molina, J., and lun Chen, W. (2004). Wireless wallet. mobiquitous, 00:32–41.

Ramfos, A., Karnouskos, S., Vilmos, A., Csik, B., Hoepner, P., and Venetakis, N. (2004). Semops: Paying with mobile devices. In I3E, pages 247–261.

Mobile FeliCa. Retrieved January 11, 2006, from http://www.felicanetworks.co.jp/index.html.

Pay Pal. Retrieved January 11, 2006, from http://www.paypal.com.

Paybox. Retrieved January 11, 2006, from http://www1.paybox.com.

Nokia Wallet. Retrieved January 11, 2006, from http://www.forum.nokia.com/info/sw.nokia.com/id/37ae0410-6e97-4f23-9a8a-c23ba7c0fd25/Wallet_Release_2_0_en.pdf.html.

Vodafone's m-pay bill. Retrieved January 11, 2006, from http://www.vodafone.co.uk/mpay.

Java 2 Platform, Micro Edition (J2ME). Retrieved January 11, 2006, from http://java.sun.com/j2me/index.jsp.

Pilioura, T., Tsalgatidou, A., Hadjiefthymiades S., (2003). Scenarios of using Web Services in M-Commerce. ACM SIGecom Exchanges, 3(4): 28–36.

Java Card 2.2 Platform Specification. Retrieved January 11, 2006, from http://java.sun.com/products/javacard.

JSR 177: Security and Trust Services API for J2ME. Retrieved January 11, 2006, from, http://java.sun.com/products/satsa.

OMA Download over the Air. Retrieved January 11, 2006, from http://www.openmobilealliance.org