An open financial services architecture based on the use of intelligent mobile devices

Apostolos Kousaridas *, George Parissis 1, Theodore Apostolopoulos 2

Computer and Communication Systems Laboratory, Department of Informatics, Athens University of Economics and Business,
76, Patission Street, 104 34 Athens, Greece

Received 16 September 2006; received in revised form 23 April 2007; accepted 25 April 2007
Available online 6 May 2007

Abstract

The scope of this paper is to explore, analyze and develop a universal architecture that supports mobile payments and mobile banking, taking into consideration the third and the emerging fourth generation communication technologies. Interaction and cooperation between payment and banking systems, integration of existing technologies and exploitation of intelligent procedures provide the prospect to develop an open financial services architecture (OFSA), which satisfies requirements of all involved entities. A unified scenario is designed and a prototype is implemented to demonstrate the feasibility of the proposed architecture.

© 2007 Elsevier B.V. All rights reserved.

Keywords: m-Payments; m-Banking; m-Financial services

1. Introduction

One of the most important steps in financial transactions is the use of a mobile device as a payment instrument and as a way to consume banking services. The continuous evolution of wireless technology, in combination with the widespread use of mobile devices, has paved the way for the fast evolution of mobile commerce and mobile financial services in particular. Although several architectures for the provision of financial services have been proposed to date [1], user acceptance and satisfaction rates remain low. Technological immaturity, early adoption of such services and users’ fear to use unmanned services are some of the facts that have limited the widespread use of mobile payment and banking systems. We were motivated to propose a new architecture by the need for a universal solution, which will not be limited to specific transactions and which will provide innovative, efficient and personalized financial services to the users, satisfying financial organizations’ and merchants’ requirements.

The aim of this work is to develop an open financial services architecture that integrates the financial services, including payment and banking ones, based on two primary capabilities: the use of computational resources of a trusted mobile device and the establishment of a user-controlled “cooperation channel” with the customer’s bank. The proposed architecture is characterized as bank-centric, since the bank acts consultatively, informatively and protectively for the end-user. Open technologies, in conjunction with standardized interfaces, offer flexibility, adaptability and continuous extendibility to our architecture.

The remainder of this paper is organized as follows: Section 2 presents the related work, the communication technologies that are involved and the existing technological limitations. In Section 3 the proposed architecture’s layered view and its significant functional requirements are presented along with the component’s description and their interactions. Section 4 deals with the implementation of a
prototype. An evaluation of our approach is also given. Finally, in Section 5 we conclude with key points and future research directives.

2. Problem analysis and related work

2.1. Related work

Various definitions exist as regards e-payments and e-banking. According to the Mobile Payment Forum definition [2], “mobile payment is the process of two parties exchanging financial value using a mobile device in return for goods or services”. The customer-to-customer (C2C) mobile payments can be characterized as a special case regarding the exchanging financial value parties, better and more accurately defined in [3]. Electronic banking using a mobile device is regarded as a sophisticated way to provide retail banking services and in comparison to traditional procedures [4, 5], has many advantages for banking organizations and customers. According to Poustchi and Schurig [6], mobile banking is divided into two main categories: mobile brokerage and account management procedures. Queue avoidance, immediacy, ease of use and low cost are some of the advantages that mobile banking offers. These advantages improve the profile of financial organizations by creating new business and marketing models. At the same time, we have to point out that any additional delivery channel has its own risk characteristics and limitations.

Karnouskos [7] and Ondrus [8] have identified several types of mobile payments considering the amount and the type of the transaction, the location of the point of sale (POS) or the payee and the number of the involved parties. Furthermore, they illustrate various payment architectures considering the means and the time of payment as well as the security level.

When designing a mobile payments and mobile banking architecture, it is necessary to take into account the following requirements [8–10]: support of every payment and banking scenario, low cost for all entities (customer, merchant and banking organization), mobile device and platform independence, minimal cooperation among mobile network operators (MNO) and financial organizations, open standards and programming languages, privacy, reliability and security, simplicity, efficiency, ease of use and integration of legacy applications.

Zhang et al. [11] describe a biometrically enabled mobile payments’ solution that uses Java smart card technology embedded into the SIM card of a mobile phone, which not only stores critical information but also executes computations. The proposed solution is a MNO centric architecture, where the MNO is responsible for distributing merchants’ public keys and for settling e-purse transactions. The user buys a SIM card that contains a unique key for data encryption and authentication, which is associated with a bank account. Saxena et al. [12] consider phone as an Europay, MasterCard and VISA (EMV) payment instrument, linked to a debit or a credit card bank account, through the use of a SIM-based security framework. SEMOPS [13] was developed in the context of a European Union (EU) funded project and is regarded as one of the most advanced universal and open payment systems. Recently, the second phase of SEMOPS (SEMOPS II) has been launched, in order to proceed with the market validation of the SEMOPS service. Labrou et al. [14] propose a wireless wallet that supports three types of financial transactions: peer-to-peer, Web store front and physical point of sale. Electronic wallet suggests a generic architecture and a new security protocol for the conduction of secure multi-party agreements. Mobile devices through their wireless communication interfaces allow provision of advanced financial services in isolated areas. This problem was addressed by our research group in the context of the EU funded IST project, named STARFISH (STate of the ARt Financial Services for the inHabitants of isolated areas) [15].

Apart from research initiatives, there are several commercial payment systems already in use. Mobile FeliCa [16] and Mobile Suica [17] are the two successful solutions that have been launched in the Asian market. Furthermore, Pay Pal [18], Pay Box [19], Mobipay [20], Nokia Wallet [21] and Vodafone’s m-pay bill [22], are also well-known commercial solutions. Finally, in order to present a complete view of mobile financial services’ environment we should point out the role of fora and standardization bodies, like Mobey Forum [23], Mobile Electronic Transactions [24] and PayCircle [25].

2.2. 3G/4G communication systems and short range wireless technologies

The third (3G) [26] and fourth generation (4G) or beyond 3G communication technologies, in combination with short range wireless technologies, like Bluetooth [27], RFID [28], IrDA [29] and NFC [30], constitute the technological background for the development of e-banking and e-payment systems, using mobile devices. These technologies influence the service provisioning context and pose constraints in the development of such systems. 2G and 2.5G [26] are still the most widely used communication systems in the world. Their main features, namely voice, Short Message Service (SMS), as well as the Wireless Application Protocol (WAP), have shaped the majority of the proposed systems [19, 20]. 3G systems [26] came to overcome the limitations and inefficiencies of the previous ones. A 3G wireless network supports numerous heterogeneous links, providing high data transmission rates and guaranteed quality of service (QoS). Almost anywhere connections provided by a multi-mode mobile device, increase the value and usability of mobile financial services. Personalized and location-based services are some of the main enhancements in 3G systems.

Research community is currently studying the fourth generation (4G) mobile network communications [31]. 4G
will offer advanced services as well as higher reliability, security and higher data rates with adaptive interfaces. The key features of the emerging 4G networks are ubiquitous computing, integration of different wireless communication technology capabilities, continuous and always best connections, seamless handovers, and all-IP network infrastructure.

One of the most important short range wireless technologies, which is expected to play significant role in the future mobile payment and banking systems, is near-field communication (NFC). According to the NFC Forum directives and standardization initiatives [30], an NFC Forum device can operate both as a contactless smart card as well as a reader of NFC-compatible tags, enabling simple and fast data transfer between NFC devices. Bluetooth and IrDA are alternative short range technologies that are able to support local or peer-to-peer payments [32].

2.3. Technology limitations vs. m-financial systems acceptance

After studying the related work and aspects, we have deduced several reasons that may have caused the obsolescence of existing architectures. Several architectures have tried to deploy software and hardware that could not – by their nature – satisfy basic requirements mentioned in Section 2.1. More specifically, many architectures were designed on top of low-speed 2G networks, which are not packet-based. The first mobile banking systems were either based on SMS service or were developed using WAP 1.0. As a result, only some fundamental services, such as account checking, were offered. Although 2.5G systems have upgraded mobile banking services through WAP 2.0 and XHTML browsers, they have not offered any substantial advancement in mobile payments area.

Technological immaturity, in combination with early adoption, usually leads a system to limited adoption and consequently to rapid decline in value. Something similar has happened in the field of mobile financial services. There are many proposed architectures, which in many cases have not met the prospective acceptance. These architectures were based on the available technologies, which were not enough evolved. Interoperability, handovers, continuous and uninterrupted connections are issues that research community should deal with, in order to achieve wide use of mobile payment and banking applications.

3. The proposed open financial services architecture (OFSA)

In this section we describe a viable and robust architecture, which provides the user with the ability to use their mobile phone as a mobile wallet, to initiate, activate and confirm financial services, including payment and bank transactions.

3.1. OFSA layered view

Fig. 1 depicts the way we conceptualize the environment, within which the described architecture is defined. The upper Transaction-related layers present the main
Financial Transaction types, as well as the Means of Payment that the proposed architecture should support. The three lower layers present a plethora of Security, Software Engineering and Communication Technologies that are available for the design and the development of mobile systems. Each technological option presents advantages, but it also sets constraints. At this point, it should be mentioned that the components of the technology layers evolve continuously, providing advanced features and satisfying new requirements. Open Financial Services Architecture is able to support this evolution due to its open approach. Finally, OFSA Functional Requirements' vertical plane presents significant features that are introduced in our architecture: trust among the involved parties (Customer, Merchant and Banking Organization), openness, intelligence introduced in the mobile device, technology integration as well as bank and payment service integration. We believe that the integration of the components that constitute the above described layers, in conjunction with the key functional requirements, leads to the design of a universal system.

OFSAs describes a system which is capable of managing financial services, including bank services and payments, through a mobile device, and offers an implementation of the so called Universal Mobile Payment System (UMPS) [10].

Interaction and cooperation between payment and banking systems as well as integration of existing technologies provide us with the ability to achieve simplicity and usability, universality, interoperability, security, trust, privacy and integration of legacy applications. End-to-end openness and the intelligence that is introduced in the mobile device are key points of our architecture.

The proposed architecture is characterized as open, since it deploys open standards for key interfaces within the system and among the involved entities. This approach can lead to a more competitive environment, where many players with different roles can co-exist. The entities that participate in an open architecture should assure their smooth collaboration, via some trust mechanism or business agreements.

The mobile device needs to make decisions and support user's actions based on user's requirements and profile (e.g., payment method). These decisions are critical for efficient transaction management. However, decision making is a complicated procedure, considering the different types of transactions and requirements. The decision component does not replace the bank's decision support system (DSS), since it acts in a supplementary manner, based on previous knowledge, user's preferences or even banks' DSS proposals. Mobile devices' intelligence should be increased, by improving decision making and support systems through a continuous learning process, using knowledge developed from previous transactions.

We have decided on a component-oriented architecture based on the following design criteria: software engineering design principles, decoupling of technological issues from business logic and facilitating the extendibility of the system. Any new business application can be implemented using either existing or future technological infrastructures, while new technologies can be deployed without affecting the existing business applications. For example, in a fully implemented system, introducing a new communication technology such as NFC (which is a continuously evolving technology) does not require any fundamental changes in the system. Minor changes in the Local Communication Component would be sufficient. Further decomposition of technology and business components supports expansion capabilities, as far as new technologies and new business models are concerned, enhancing OFSA openness. For instance, if an alternative security scheme (e.g., from Kerberos to PKI) is required by the bank, only minor changes in the Security Component will be necessary.

### 3.2. OFSA functional requirements

Considering the technological environment, the involved entities' requirements, the already proposed architectures and the aforementioned systems' acceptance factors, we can proceed with outlining the features of the proposed architecture. The composition of functional requirements for the development of an open mobile financial services' architecture, taking into account the prerequisites for wide acceptance and the potential risks, is considered as a very complicated task.

The prime principle of our architecture that defines the context in which we set its functional requirements is the trust factor built between user and banking organization and between user and her mobile device. Traditionally, people trust financial organizations, since they offer security and guarantees to every transaction and have built the necessary reputation. For that reason, our architecture is designed to be bank-centric, since we believe that this would be a factor that favors wide user acceptance. Using the term bank-centric, we illustrate the role of the bank as the main control and coordination point in every financial transaction.

Furthermore, we regard system integration as a significant functional requirement that is taken into consideration in OFSA design. In the majority of the proposed architectures, e-payment and e-banking systems operate as two separate applications for the end-user. We consider integration of payment and banking systems as necessary, especially for ubiquitous computing environments, where transaction procedures are complicated. It is not a simple integration of the corresponding applications, but an integration of business layer procedures. 3G and emerging 4G communication technologies create new potential for financial systems development and, at the same time, they offer
innovative, ubiquitous and pervasive services that affect the requirements both quantitatively and qualitatively [33]. The technology integration factor was taken into serious consideration when designing the proposed architecture, as well as when integrating financial transactions to one device, which provides unified management. Technology integration involves the unification of various technologies supporting same functionality, through the deployment of discrete components. For example, communication technologies such as UMTS, Wi-Fi and WiMAX are grouped together and managed by the Remote Communication Component, through a unified way.

OFSA architecture does not only focus on user oriented requirements but also takes into account financial organizations’ ones. Thus, one of the main architecture’s functional requirements is the exploitation of current infrastructure and software, which decreases system’s development cost and allows easy adoption. We satisfy this requirement by using the Web services technology. Another requirement set by financial organizations, and satisfied in the proposed architecture, is the capability to provide personalized services. This capability increases a user’s utility and, in parallel, enables banking organizations to adapt their services, according to a user’s profile, needs and characteristics, thus increasing their profit.

Security is one of the most important requirements that involved entities set. In such systems, where crucial data are transferred and payment transactions are taking place, security mechanisms as well as secure communication protocols must be implemented in every stakeholder. Thus we have faced security as an end-to-end issue. Security, as a requirement, is the provision of confidentiality, integrity, authentication, authorization, assurance and non-repudiation in every transaction. Critical data involved in financial transactions must be stored securely in the mobile device or in the bank’s storage infrastructure. Smart cards, embedded or external, are security elements that ensure secure storage of information, so that non-authenticated applications or users cannot retrieve and use this information. They also provide a secure environment for computational process execution. One important issue is to define the actors who can store information in these security elements and the information category that each actor is responsible for. For instance, the device’s owner can load electronic coins on the smart card through an ATM. On the other hand, certificates and private keys for asymmetric encryption of bank transactions are exclusively loaded by the banking organization.

The above-mentioned information can be stored either in the USIM or in a NFC chip. As mentioned in Section 2.2, the main advantage of NFC chips, which have three different operation modes [30], is that they can even work when a mobile device is deactivated (e.g., due to a power shortage). In this case, an NFC chip can operate as a contact-less smart card, independently from the mobile device, supporting specific operations like the execution of mobile payments.

3.3. OFSA component analysis and interaction

Component-based design of OFSA offers extensibility characteristics and enables developers to introduce advanced functionality and services or improve existing ones. Before we proceed with the architecture components’ detailed analysis, we present an overall view (Fig. 2), which focuses on the mobile device side and the interfaces that the latter exports to other entities, including banking organizations, points of sale, smart cards and peer mobile devices.

Fig. 3 presents the components that constitute OFSA on the side of the mobile device. These components interact with each other and with the bank and POS OFSA entities through internal and external open interfaces, respectively.

The User Interface Component is responsible for the presentation of the information to the user, through a series of displays and interactions. When designing OFSA, we tried to separate the presentation layer from the business and application logic, thus OFSA is able to support multiple mobile devices in terms of input and output capabilities. This component is also responsible for the interactions between user and application, offering techniques and software tools that facilitate information entering. According to the user’s actions, it sends signals to the Control Component through the corresponding ‘Control Interface’, which coordinates the necessary procedures. On the other hand, its exposed ‘Presentation Interface’ is used in order to present the appropriate information with the suitable format.

The Control Component undertakes the coordination of the procedures and the internal interaction of components. It also allocates received messages to the appropriate internal component. Local and Remote Communication Components forward received messages to the Control Component, through the ‘Control Interface’. Further on, the Control Component dispatches each message and triggers the appropriate component, as regards the next procedure. In sequence, the Control Component is also triggered by the other components, through the same interface. Final
actions for the Control Component might be the trigger of the User Interface Component to present some information, the request to the Local or Remote Communication Components to transmit messages to other OFSA parts or the execution of an internal procedure. For instance, if the Remote Communication Component has received an encrypted message from the issuer, this message is transmitted to the Control Component. The former decrypts the message first by utilizing Security Component mechanisms, and then identifies that it is an alert message. Thereafter it informs the user about a suspicious account change. Finally, the Control Component immediately notifies the ‘User Interface’ to present the message at the device screen.

The Decision Component is responsible for decision making on the client side. This component introduces intelligence to the device, which is aware of its owner’s preferences and generally the environment that the user is placed in. It consists of two subsystems; a local DSS and an agent that communicates with the bank’s DSS. It is responsible for the decision making when the application must consider various requirements or parameters, in order to make a financial transaction. For instance, when a user buys a product from a physical POS, this component should propose the appropriate payment method, considering the means that are accepted by the merchant. The mobile device DSS, in cooperation with the corresponding component of the bank, is able to provide personalized services. For example, urgent messages alert the user for unusual or suspicious transactions. Moreover, statistical reports help the user to efficiently use her mobile phone as a personal consultant. The decision making could be potentially extended using sophisticated techniques, like artificial intelligence algorithms. For thin mobile devices simple rules that are defined by the issuer and the user are considered as adequate.

The Payment Component includes the necessary algorithms for account or credit card-based payments as well as algorithms for digital cash transactions. The aforementioned methods provide all kind of payment means that the user selects to activate, offering the device with the ability to execute peer-to-peer money transfers and mobile payments remotely to a virtual POS or locally to a physical
POS. The open approach of OFSA allows the implementation of various payment schemes (e.g., VISA 3D-Secure, MasterCard SPA). Through the ‘Payment Interface’, the Control Component calls the appropriate functions in order to initiate the payment procedure, taking into account the Decision Component’s proposal regarding the specific transaction. According to the type of the transaction and the payment scheme, the mobile device Payment Component interacts with the respective components on the side of the issuer (Payment Services Component), the POS (Transaction Settlement Component) or a peer mobile device (Payment Component).

The Banking Component undertakes control of the application, when transactions with the banking organization should take place. Accounting and personal information, bank transfers, investments and application forms are some of the services that user can experience through this component. As mentioned above, one key point of the proposed architecture is the interaction and cooperation of payment and banking subsystems. OFSA achieves integration of these two subsystems, by allowing their intra-communication. A purchase from an unmanned POS through a bank transfer is a representative example. The Banking Component cooperates with the respective Component (Banking Services) on the side of the bank (issuer).

The Trust Mechanism is introduced in order to increase consumers’ and merchants’ confidence, protecting them from users that are not legal and fair. Establishment of trust enables user and merchant to transact even without the intervention of administrators, who authorize these transactions. During a payment transaction, the payment scheme that is used provides the first level of confidence among the involved parties. The bank (Acquirer) guarantees that the payee (merchant) will receive the money from the payer and the transaction can conclude successfully. In addition, the trust mechanism could be used to inform and protect the involved parties about other aspects of the transaction, such as low quality products and services or fraudulent payments. In the context of electronic payments, many trust theories are based on the history of the transactions that each entity (mobile device user, POS) has conducted, but only several trust metrics have been introduced to date [34]. The type and value of the transaction may specify the trust level that the involved entities demand. A trusted third-party (TTP) could be used to provide trust and ensure that the involved – in a payment transaction – entities, are not malicious. The role of the TTP could be assigned to the financial organization or to an external, well known and trusted organization. TTP is informed by mobile device’s Trust Mechanism about negative behavior that an entity had, affecting its trustworthiness.

Furthermore, the Trust Mechanism should be able to locally collect information about entities that have, for example, frequent transactions. The presence of this component becomes more important in the case of peer-to-peer payments. The Decision Component, through the defined ‘Trust Interface’, requests a response about the reputation that a peer entity or a POS has. The Trust Component can communicate with the corresponding mechanism on the side of the TTP and evaluate the trust level of the respective entity.

The Local Communication Component handles communication between physical POS and the mobile device or between peer mobile devices. Payment messages can be physically transmitted via various air interfaces such as Bluetooth, IrDA or NFC, depending on the hardware and software features of the mobile device. This component implements Bluetooth, IrDA or other short range technologies APIs. It retrieves messages that arrive from the corresponding short range interface and forwards them to the Control Component. The ‘Transfer Interface’ defines operations for the transmission of messages to the POS or peer entities that use short range wireless technologies. This component communicates with the corresponding component of other peer mobile devices and with the Mobile Device Communication Component on the side of the merchant.

The Remote Communication Component controls the mobile device’s communication, when a remote transaction, such as the provision of a retail banking service and/or an Internet payment, is taking place. Communication technologies involved in such transactions are UMTS, Wi-Fi and WiMAX. The OFSA modular design permits the introduction of new technologies if needed, without the interference of other components. This component has also undertaken Web services management, including transmission and reception of SOAP messages, by utilizing XML parsers for XML message composition and decomposition. This component cooperates with the corresponding Mobile Device Communication Component, on the side of the issuer and the merchant, in case of mobile payments. The ‘Transfer Interface’ defines operations for the transmission of banking service messages to the issuer and messages in case of remote mobile payments (e.g., an online Internet shop).

The Synchronization Agent handles all synchronization actions between the mobile device and the bank server. It consists of the Synchronization and the Update Subcomponents. The first one allows mobile device and bank to cooperate, in order to periodically synchronize their common data (e.g., transaction history files, e-receipts) and also provides the mobile device with a back up storage place. A secondary repository provides additional security and an alternative way for the user to access information and services (e.g., through a web browser). Furthermore, through the ‘Synchronize Interface’, the Control Component may request transmission of e-receipts that are stored locally in the remote database of the issuer. Moreover, the Control Component through the ‘Request Updates Interface’ (Update Subcomponent) is able to request updates about components that the bank is authorized to handle. The Update Subcomponent contains an agent for the over
the air (OTA) download and management of OFSA components. For instance, the bank is able to update the Payment Component by adding a new payment scheme or the Banking Component by including a new bank service. Furthermore, a new security scheme or feature can be downloaded. The Synchronization Agent collaborates with the Remote Management Component, on the side of the issuer, which has the ability to initiate an update procedure.

The Smart Card Management Component implements the mechanisms that manage and control smart cards, either external or embedded into the mobile device. The latter may interact with various types of smart cards, exploiting their capabilities. Each smart card type is handled by the corresponding subcomponent: the USIM Subcomponent undertakes to communicate with USIM and utilize its exported functions. The NFC Subcomponent manages the NFC chip [30] and the External Smart Card Subcomponent handles external smart cards, in case that the mobile device incorporates the relative reader. The Smart Card Management Component is responsible for the retrieval of information that is stored in the smart card as well as for the call of functions, which are exclusively executed by the smart card microprocessor. The ‘Retrieve Data Interface’ defines the operations for the insertion, retrieval and update of data stored in the smart card. Furthermore, the ‘Execute Interface’ defines operations that are executed in the smart card, such as encryption/decryption of sensitive data, secure logon and authentication of users. The Control and Security Components are the only components that can directly communicate with this interface.

The Security Component includes the mechanisms that are necessary for user’s local authentication procedures and for assuring secure communication between the mobile device and the bank as well as between the mobile device and the POS. The Control Component is able to call the ‘Authenticate/Authorize’ and ‘Encrypt/Decrypt Data’ Interfaces acting as an intermediate between the rest of components and the security one. Internet applications ensure communication security using Secure Socket Layer (SSL), Transport Layer Security or Wireless TLS (WTLS) for wireless communications. PKI infrastructure and several secure XML protocols, like XML digital signatures, XML encryption and Web services security protocol family, are some of the alternative popular security approaches [35].

Communication with the banking organization (issuer) is usually implemented using a specific and predefined security mechanism. The user should be authenticated to access the banking organization when she wants to make a payment through the issuer or to use a bank service. Further on, data transmission should be confidential. The mobile device may transact with several POS or peer mobile devices, which may implement different security schemes. This makes security issues complex, since these types of communication require minimum exchange of crucial information. The OFSA security component integrates the security schemes that the issuer or any other stakeholder requires, in order to provide the entities that participate in a transaction with a secure interface.

Fig. 4 presents the OFSA Components on the side of the banking organization, which operates either as an issuer or an acquirer, or both. OFSA is designed to exploit financial organizations’ legacy applications and to support current and ongoing financial procedures. OFSA is designed to operate on top of current financial information systems, without requiring banks to change their fundamental procedures and their expensive infrastructures.

Mobile Device and Merchant Communication Components provide the mechanisms for communication between the bank and the mobile device and the merchant, respectively. These components export a ‘Transfer Interface’, which is used by the Control Component, in order to transmit data. Mobile Device and Merchant Communication Components interact with the Remote Communication Component on the side of the mobile device and with the Bank (Acquirer) Communication Component on the side of the POS, correspondingly.

The Control Component coordinates the communication among the components and the sequence of the procedures during a financial transaction. The functionality of this component is similar with the above described Control Component on the side of the mobile device. The Decision Component acts as an intermediary between the bank’s DSS and OFSA. XML adapters can be used so as to enable the Decision Component to export the available decision support services of the bank. They provide information to the corresponding Decision Component on the mobile device or on the merchant side, facilitating their decision making procedures (e.g., suggestions and potential threats).

The Security Component undertakes merchants’ and mobile device’s authentication and authorization to the acquirer and to the issuer, respectively. It also provides mechanisms for data confidentiality. This component cooperates with the corresponding Security Component on the POS and on the mobile device side. The Bank Services Component includes the necessary procedures for the settlement of bank transactions after user’s request. This component cooperates with the core bank information system. For instance, in case of a bank transfer, Bank Services Component, following Control Component’s signal, forwards the request to the appropriate module of the core bank information system. The Payments Services Component is responsible for the transfer of money from the payer to the payee and for the settlement of the payment orders. It includes the payment schemes that the issuer supports and also allows the implementation of new or extended payment models, as the one which is described in the scenario section.

Trust Mechanisms provide bank with the ability to create a trust network, where customers and merchants will be protected from unfaithful entities, while fair users will be identified and have more profitable services and products. The bank may operate as a trusted third-party (TTP) and thus it can be informed by POS or mobile...
devices about fraudulent events. Finally, the Remote Management Component includes all these functions that enable the bank to manage and control OFSA procedures on the merchant or on the mobile device side, to provide updates and to share information.

The last two components as well as the Decision one are key points for implementing the cooperation channel between the bank and the mobile device. The Trust Mechanism is utilized by the decision making mechanism, while the Remote Management procedures are triggered by the Control Component through the ‘Update Interface’, after an internal bank decision or after a mobile device’s request (Synchronization Agent).

Fig. 5 depicts OFSA on the merchant side that can be either virtual, (e.g., Web store front) or physical (e.g., vending machine). The Mobile Device Communication Component is responsible for the communication between the POS side of OFSA and the mobile device during a purchase. The Bank (Acquirer) Communication Component is responsible for the POS communication with the bank (Acquirer), so as to settle a payment or to provide value added services. These two components contain the necessary software mechanisms for messages’ reception and transmission, using the communication technologies that the POS supports. The Control Component utilizes their ‘Transmit Interfaces’, in order to send messages to the mobile device or to the acquirer.

The Merchant Configuration Component provides an external interface that enables merchants to manipulate their POS, by modifying various transactions’ parameters (e.g., product prices). The Control Component, as described above, is triggered through the ‘Control Interface’ by the rest OFSA components, in order to coordinate the interactions among the components in the context of a payment transaction.

The Decision Component, which is signaled through the ‘Decide Interface’ by the Control Component, evolves POS functionality, making its decision process more intelligent. For instance, the ability to adapt parameters of the transaction, like the price or the discount, according to purchase’s context, user’s transaction history and the level of trust is an example of decision making on the POS side.

The collaboration of the Decision Component and the Trust Mechanism, through the ‘Trust Interface’, enables
the POS to check the level of clients’ confidence. The Trust Mechanism cooperates with the respective component on the side of the trusted third-party banking organization and, apart from checking transacted entities confidence level, has also the ability to inform the TTP about malicious transactions or clients.

The Transaction Settlement Component, which is triggered by the Control Component through the ‘Payment Interface’, cooperates with its acquirer Payment Services Component and with the mobile device Payment Component, so as to settle a pending payment. Finally the Security Component through its exported ‘Authenticate/Authorize’ and Encrypt/Decrypt Data’ Interfaces provides POS with the ability to secure the communication with the mobile device and its acquirer.

4. Mobile payment scenario using OFSA prototype

4.1. Scenario description and transaction flow

In this section, we describe a sophisticated financial service scenario where payment and banking services are combined and a home-grown payment scheme is deployed. Throughout the scenario description, we have attempted to illustrate the inter-component interactions, as well as their internal functionality.

A user wants to buy a product from an unmanned Bluetooth-enabled POS, using her intelligent mobile device. The user selects the desired product, by physically interacting with the POS. The POS provides several ways for the payment including e-coins, bank transfers and credit or debit cards. The user, taking into account the bank’s and the mobile device’s suggestion, selects to pay through her debit card and initiates the payment procedure using her PIN. After payment is completed, the user takes the product that she has bought and the e-receipt that proves the conducted financial transaction. Fig. 6 depicts the interactions among entities and the sequence of messages which are necessary for the aforementioned transaction.

The user selects the desired product (step 1) and holds her mobile device near merchant’s Bluetooth interface, in order to initiate the transaction. The POS through the ‘Mobile Device Communication Component’ transmits transaction’s information to the mobile device (step 2),
including: Transaction’s unique ID, Transaction’s Timestamp, Product’s Information and POS Information (Fig. 7).\(^4\)

The ‘Local Communication Component’ on the mobile device side receives the transaction’s data, which are forwarded to the ‘Control Component’. The latter identifies the type of the transaction and coordinates the next steps. First of all, transaction’s information is presented to the user through the ‘User Interface’. The user checks its validity and accepts the purchase. Before payment’s initiation, the ‘Control Component’ requires user’s local authentication. The user inserts her PIN (step 3) at the appropriate form of the User Interface and thereafter the ‘Security Component’ undertakes the local authentication procedure. This component triggers the ‘Smart Card Management Component’ to call the corresponding function at the smart card so as to authenticate the user (steps 4–6). Upon the user’s authentication, the ‘Security Component’ informs the ‘Control Component’, which in sequence requests the ‘Decision Component’ to identify the most appropriate payment method (step 7). The mobile device ‘Decision Component’ requests bank’s suggestion (bank’s ‘Decision Component’) via ‘Remote Communication Component’ and ‘Mobile Device Communication Component’. After the user’s authentication by the bank (steps 8 and 9), the mobile device transmits the encrypted transaction’s information (Fig. 8). The bank, taking into account the amount of the transaction, the user’s transactions history, her account balances and her preferences, proposes the appropriate payment method (Fig. 9) for the specific transaction (steps 10 and 11).

After receiving the bank’s suggestion of a payment method, the mobile device’s ‘Decision Component’ filters and gives final verification for the payment method’s validity (step 12), the user selects the payment method (in this case her debit card) and initiates the payment procedure (step 13).

The mobile device via the ‘Local Communication Component’ informs the POS (‘Mobile Device Communication Component’) about the selected payment method (step 14). In the sequence, the mobile device’s ‘Payment Component’ completes the payment procedure by interacting with the POS (‘Transaction Settlement Component’), taking into account the payment scheme that the merchant uses. For this specific scenario, the POS uses an e-payment scheme, where the payment is accomplished via the customer’s

---

\(^4\) An XML schema can be viewed as a directed graph where the vertices correspond to elements or attributes and the edges represent containment (parent–child) relationships. The vertices are labeled with the name of the element/attribute. The edges have an additional multiplicity label that is presented using the asterisk (*) symbol [36].
issuer bank and POS acquirer bank. The POS asynchronously informs its acquirer that a payment is pending. The transaction is identified through the generated unique ID number (step 15) that is sent by the POS (Transaction ID). The mobile device ‘Payment Component’, via the ‘Control Component’, requests and retrieves the debit card information, which has been encrypted and stored in the smart card (‘Smart Card Management Component’) (steps 16–18). The mobile device communicates with the issuing bank, and over UMTS or Wi-Fi communication network, requests issuer (‘Payment Services’ Component) to charge the debit account (step 19). The issuer processes the request (step 20) and confirms or not – in real time – the pending transaction to the POS acquirer (step 21), which in turn informs the POS if the customer is accepted or not (step 24). The actual financial settlement is taking place according to mutually agreed business rules. After acquirer’s confirmation (step 22) the issuer informs the mobile device (‘Payment Component’) that the transaction has successfully concluded (step 23). Finally, the POS delivers the product (step 25) and the corresponding electronic receipt (step 26) to the mobile device.

4.2. Prototype outline

We have implemented an OFSA prototype, which focuses on the mobile device side and on the cooperation channels that this device can accommodate with other entities, including banking organization, POS, smart card and peer mobile devices, as depicted in Fig. 7. We have successfully tested the aforementioned unmanned POS m-payment scenario in a semi-emulation environment [37]. For the purpose of the scenario, we have implemented a virtual bank and a virtual vending machine (Point of Sale). Fig. 7 illustrates the involved entities and the mapping of the main technologies that have been selected. The mobile device application has been implemented using the smart client model, and specifically the Java 2 Micro Edition (J2ME) programming language. We have used the Sun Java Wireless Toolkit to emulate the mobile phone (see Fig. 10).

Mobile Web services [38] is the technology that has been used for the implementation of communication among the mobile device, the POS and the bank application server.
Web Service Description Language (WSDL) and XML Schema Definition (XSD) files describe the operations and the services that the banking organization and the POS offer to the mobile device as well as the messages and data types, exchanged between these entities. Financial services are invoked over the WWW using Simple Object Access Protocol (SOAP) messages, which are XML-based, and are used for the implementation of communication between the involved entities. JSR 172 Web services API (WSA) [39] allows a J2ME-enabled mobile device to request Web services, by providing XML parsing capabilities using Simple API for XML (SAX2) and XML-based Remote Procedure Call using JAX-RPC. Further on, on the bank and POS sides, an Apache Axis server is used for Web services provision and execution. Regarding peer-to-peer communication, Bluetooth technology is used and more specifically the JSR-82 API [40], which provides Bluetooth capabilities to J2ME-enabled devices.

Critical information is stored and operations are executed in Java Card USIM, where Java Card applets are implemented using Java card platform [41]. For the communication between the mobile device and the smart card we have used the “Security and Trust Services” API (SATSA) [42]. Moreover we have tested the integration of the mobile device and Kerberos [43], which has been used for user’s authentication and authorization. The Key Distribution Center (KDC) consists of the Authentication Center for user’s authentication and the Ticket Granting Server (TGS). The latter issues tickets for the communication between the bank application server and the mobile device.

More information with regard to the prototype, the defined WSDL and XSD files, as well as screenshots and implementation details, is available at the OFSA implementation Web site [37].

4.3. OFSA discussion and evaluation

The prime OFSA feature is the integration of payment and banking systems as well as the establishment of a
proposing specific services or actions according to her preferences. OFSA introduces intelligence in the mobile device and deploys the exported banks’ business intelligence and decision support services. The mobile device’s rule-based Decision Component operates consultatively on behalf of the user, proposing specific services or actions according to her profile, preferences and history of transactions.

Moreover, most of the proposed systems are based on specific payment schemes [7]. OFSA, however, is not bound to any payment model, since the mobile device ‘Payment Component’ is extensible to support any payment model. The Over the Air download mechanism allows a mobile device to download payment schemes and services from the issuer.

Hardware, operating system and programming language independence have been key requirements in the design of OFSA. Service oriented architecture, which is implemented with Web services, supports language independence and assures the desired platform interoperability and openness.

Many of the up-to-date commercial systems are based on SMS, voice or WWW [7]. On the other hand, OFSA as well as [11,14], adopt the smart client model for developing applications on the mobile device side. The main features of the smart client model are mobile device autonomy, extensibility and facilitation of mobile device resources’ control. Furthermore, offline browsing, which is supported by the smart client model, enables user to access mobile financial services while avoiding continuous interaction with the remote server.

Moreover, regarding security issues, Zhang et al. [11] propose the usage of the USIM card in order to implement user authentication or encryption/decryption of transmitted messages. OFSA supports information storage, like electronic receipts and transactions’ history file, on a remote repository, which could be either on the issuer side or on a trusted third-party. It also supports critical information storage (e.g., PIN, or credit and debit card information) on portable smart cards. Thus, the user has the ability to access her information from various devices and locations, which are considered as secure.

Storing information in the handset and especially in the NFC chip is an alternative for securing crucial data. The GSM Association (GSMA) [44], the global trade association for mobile network operators, is participating in the NFC initiative to encourage common specifications in implementing NFC technology in mobile phones.

On the other hand, the transmission of personal data to the issuer and the cooperation channel itself may raise privacy issues. In order to overcome these issues, mechanisms for the provision of anonymity must be provided. Furthermore, in many cases, only MNOs are authorized to load and install applications in the USIM card. This means that there is a need for cooperation between the bank and the MNO. Additionally, the cost that arises when data transmission occurs from the bank to the mobile device and vice versa is an issue that should be taken into account in the cooperative relationship between MNOs and banks. An innovative business solution that combines banking activities with mobile telephony is the Mobile Virtual Network Operator (MVNO) service, which is owned by banking organizations. This model allows the MVNO to control the USIM card and to use various pricing policies. Finally, while OFSA can be easily implemented for a virtual POS, the upgrade of physical vending machines is considered as a more complex and costly aspect, since these machines are mainly hardware-based.

During the prototype implementation and testing process [37], we have pointed out some important aspects that are worth mentioning. Firstly, the development technologies (e.g., programming languages-J2ME, wireless toolkits) for mobile device applications are still immature enough to create a stable and ready for production project. A lot of interoperability and compatibility issues arise between the different versions of the above products. Furthermore, introducing advanced functionality to a mobile environment, which supports limited computational and network resources, is not always a trivial procedure. In the case of OFSA, maintaining the component design on the mobile device side has been a difficult task, especially regarding the security mechanisms. These are still in a primitive state.

5. Conclusion

In the present paper, we have identified the main requirements that mobile financial systems should satisfy and we have discussed the main reasons that caused a low-level of user acceptance of already developed systems. We have described an Open Financial Services Architecture which satisfies the involved entities’ requirements and provides innovative features. Technology integration, platform independence, openness, intelligence and trust among involved parties are OFSA’s main characteristics. Furthermore, OFSA proposes payment and banking systems integration as well as the establishment of a cooperation channel between the mobile device and the banking organization. The described scenario and the corresponding implemented prototype support OFSA’s presentation and demonstrate its feasibility.
Our ongoing work includes further testing the implemented prototype and extending its functionality. The final prototype implementation should be benchmarked to evaluate OFSA and assess its performance. For that reason, we intend to thoroughly investigate potential quantitative and qualitative criteria and metrics.

Acknowledgements

We thank Mrs. Kefala for her helpful comments and her contribution during the editing phase. Furthermore, we also wish to thank the E-Commerce Research and Applications m-payments special issue editors, Robert J. Kauffman, Stamatis Karnouskos, Elaine Lawrence and Key Pousttchi as well as the anonymous reviewers for their constructive suggestions and comments during the whole revision process.

References