

SYSTEM OF MEDIATION FOR MOBILE PAYMENT WITH THREE FACTORS AUTHENTICATION

¹WADII EL HILLALI, ²JAOUAD BOUTAHAR, ³SOUHAÏL EL GHAZI EL HOUSSAINI

¹ Department of Computer Science, ENSEM, Morocco

² Department of Computer Science, EHTP, Morocco

³ Department of Computer Science, EHTP, Morocco

E-mail: ¹elhillaliwadii@gmail.com, ²Jaouad.boutahar@gmail.com, ³elghazis@gmail.com

ABSTRACT

Since the early ages, the human being has not ceased to develop its system of exchange. The first system introduced is barter which has evolved over time in currency, taking various forms (shells, teeth, feathers ...). The appearance of microelectronics has favored the appearance of a new era of payment systems which is the credit card, it is currently the most used means of payment throughout the world. Today financial institutions want to replace the credit card by mobile phone. In this article we will present the implementation of a mediation platform for mobile payment, and we will present an implementation approach to the Fido standard for Three-Factor Authentication.

Keywords: *M-payment, 3FA, NFC, Fingerprint, Android, SOAP*

1. INTRODUCTION

When Martin Cooper had designed the mobile phone in 1973, it be to make possible the telephone calls outside, it forever thought that its invention was going to be useful in a few years' futures in means of payment of very high level. When the basic features of a mobile phone have been reached, the financial institutions were beginning to offer new mobile-based business services [1], thanks to the evolution and the emergence of mobile technologies.

The evolution of telecoms networks, especially mobile internet has made accessible remote services, the customer can now from his phone, pay his bills, or buy products. The mobile payment is now more interesting than online. Now we can see that the supplier's services are more attractive than ever, a merchant can offer discount coupons or loyalty points, for example, by a simple mobile application, in contrast to physical loyalty cards, secondly, the customer can take as criterion of purchase the proximity of the merchant thanks to the GPS chip on her smartphone, it can also receive notifications on new offerings, M-commerce is supposed to replace the E-commerce in the years futures [2].

In this article, we present the steps of implementing a mediation platform for mobile payment based on Web services, it allows the

customer to automate payment of all of its fees (Water, Electricity, Telephony, taxes ...) in a single operation through a mobile application. Today, each provider offers its customers a mobile payment application, the customer then finds himself in front of several applications serving all the same, and he is forced to each to enter his personal information or use his card Bank for the payment of its royalties. We can conclude that the main objective of mobile payment has not yet been reached and we are faced with E-Commerce websites encapsulated in a mobile application. We propose to set up a mediation system connected to all the suppliers and which allows the customer to pay all his fees in a single operation automatically and without using his bank card.

We will also show that the mobile is able to offer a very high level security system by implementing a three-factor authentication of the FIDO standard, thanks to the NFC chip and the fingerprint.

A description of the detailed architecture of the platform was exposed in a first article called "Architecture of a system of mediation for the mobile payment".

2. RELATED WORKS

Manuscripts Research on electronic payment systems has inspired many researchers. Even the major players in finance (Visa, MasterCard ...) are still interested in developing

new electronic payment solutions to offer new services to their customers.

It would be difficult to consolidate literature at the level of a single discipline, as several fields of research are concerned with this field, notably business, management, marketing, engineering, information technology (IT) and information systems (IS) [16].

One can easily conclude that the progress of the research is in this field and reciprocal to that of the development of technologies. With the emergence of mobile telephony, research has focused on the implementation of mobile money transfer architectures, among them we find Jerry & Krishnaveni [17] (1), Ashutosh and Manik [18] (2).

(1) Jerry & Krishnaveni [17] propose a mobile P2P money transfer system, by setting up a secure communication protocol between the seller and the buyer,

(2) Ashutosh & Manik [18] offer a mobile payment architecture to replace credit card information by saving the EMV chip on the SIM card.

Subsequently, thanks to the emergence of the Internet and smartphones, the researchers were interested in Mobile Commerce, benefiting from advanced mobile technology (GPS, fingerprint, OS...) and a robust telecom infrastructure And more and more evolved (3G, 4G, ...).

Currently research is focused on Mobile Contactless Payment, several researchers including Rahul & Shubham [28] propose an ecosystem for mobile payments via NFC.

We have analyzed several mobile payment platforms proposed by various researchers and found that it would be difficult to implement some of these solutions in reality because these solutions do not take into account the Encounter payment solutions in the real world (Time Out, portability ...), we also found that these solutions always use the credit card as a payment medium, not taking advantage of the ability of the mobile to replace the bank card.

3. DESCRIPTION OF THE TRADITIONAL INTERACTION FLOW OF A PAYMENT OPERATION

Figure 1 represents the logic diagram of a normal flow of an electronic transaction of payment which can be summarized in four components:

Cardholder: It is the customer owning the credit card, the secret information of the card is stored either on a magnetic tape, on a SIM card, or on an NFC chip (the case of the last bank cards).

Issuer: The issuer is generally the financial institution (for example, a bank) that has made available to its client (cardholder) a payment medium (the credit card), the issuer also undertakes to Validation of a payment transaction (by verifying the identity and balance of its client) following an authorization request received from the buyer.

Merchant: Also called acceptor, which accepts electronic means of payment for the purchase of its products.

Acquirer: It is generally a bank, it is the financial institution which makes available to its client (The merchant) the services of acquisition for the electronic payment, Example: The terminal of electronic payment (POS). The Acquirer provides interfaces to the interbank networks (Visa, MasterCard, American Express ...) for the processing of payment requests, it also guarantees the clearing operation to reimburse the merchant at the end of the day for example.

In this model, the role of the acquirer is limited to a payment channel, and in no case intervenes in the business logic of the merchant. Also, for each payment transaction, the acquirer receives a percentage of the transaction amount from the merchant.

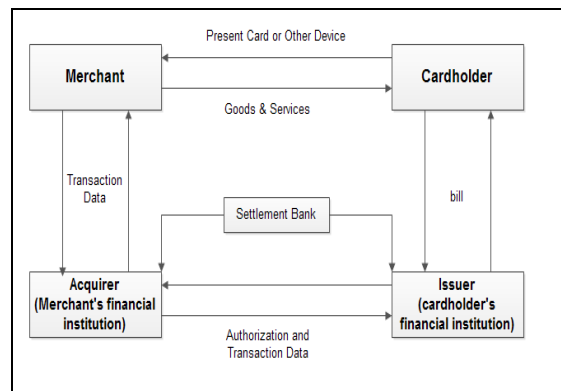


Figure 1: Typical electronic payment scenario

4. DESCRIPTION OF THE INTERACTION FLOW OF A TRANSACTION PROPOSED BY THE PLATFORM

In a payment transaction, the cost of a transaction depends on the banking networks for which this transaction is conveyed. As long as the number of these networks increases as much as the cost of the transaction is increased, each actor receives a percentage of transaction costs, and blow a question is posed on the profitability of the transaction, certain merchant refuse the credit card payment for the transactions of small amounts. In our case, we propose to reduce the number of actors in a payment transaction, the platform undertakes intermediary between the customer and the service providers/merchant, also the customer is not obliged to have a credit card, but the platform offers an internal virtual account that the customer can reload and make payments from this account. Compensation is made only between the platform and the suppliers without the customer's introduction. If necessary, the customer can use his credit card either to recharge his virtual account to make payments, or he can save the secret information of his credit cards in the platform in a secure manner if he wishes to make its payments easier.

In addition and to respect the international banking standards in term of execution time of a transaction, we conceived the architecture of our platform according to two levels (Figure 2), a part Back Office and another Face Office.

The “Front Office” part: This part is composed of several modules allowing the management of a payment transaction in real time. The first module of this section recovers all the customer's royalties from its suppliers (electricity, water, telephony, tax, etc.), after validation of the customer, another module is responsible for supplying the transaction costs via the Means of payment of the customer (internal virtual account, registered credit card, entry of a new credit card), the platform proceeds to pay all the customer's fees to all the suppliers, the detail of each invoice is Stored in a database, this data will be used by the back office for the compensation operations between the platform and the merchant. In the end the platform notifies the customer by (SMS / email) of the completion of the transaction.

The “Back Office” part: This part manages clearing operations between the platform and the suppliers, in the banking sector these operations are called "Clearing". These operations are usually done at the end of the day so as not to impact the performance of the production servers, it is to generate the accounting reports based on the transactional logs stored in the database. These logs will be the payment medium of the suppliers from the customer account.

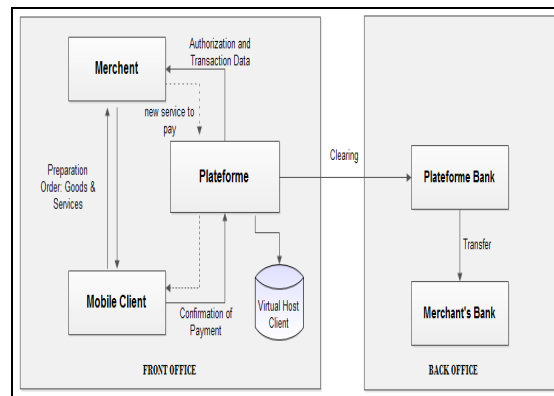


Figure 2: Proposal electronic payment scenario

5. GLOBAL DESCRIPTION OF THE PLATFORM

The platform offers an alternative electronic means of payment, especially in developing countries where access to banking services is low. The economic model targeted by the platform is that of the payment microphones, this model allows the purchase of services or contents more or less of low unit value [3]. The platform aims to solve the limitations of traditional payment systems:

- Electronic payment:
 - Reserved for people with bank accounts.
 - Security issue related to entering credit card information (PAN, Date Expiry, and CVV) on the Web.
 - Costs of transactions.
- POS Payment:
 - Requiring customer relocation.
 - Requiring sometimes a physical identification by ID card.

The architecture of the platform is based on the use of the virtual accounts, allowing customers not having a bank account, or not wishing, for safety

reasons, to use their credit card like means of payment. It offers to client three payment methods:

- An internal virtual account that can be recharged by credit card or via money transfer establishments (Western union,).
- A credit card.
- An interface, enabling to save the credit card in a secure way, the client is limited to selecting the bank and the payment is done automatically.

The platform is based on a mediation system connected to the different partners via web services, the customer starts by configuring the desired means of payment, the platform proposes by default an internal virtual account that the customer can reload via a menu, Customer has the possibility to save as many credit cards as he wishes. The second step is to configure the desired services by pulling down a list of partner vendors for the platform and entering its credentials for each service.

On the other hand, we found that the main problem with this type of platform is that the use of the balance of the portfolio is limited, once the client recharges his account, it is no longer possible to recover his money, he is obliged to consume its balance only on the services of the platform. This is the reason why many micro-payment platform have failed to attract customers. On our part, we have designed our platform in such a way as to operate as a traditional payment channel, which the customer can choose when purchasing on the E-Commerce sites.

In terms of security, the platform offers the client a means of physical authentication via an NFC card or by fingerprint for the validation of payments.

6. USE CASES

The overall architecture and use cases of the platform were published in a first article called "Architecture of a mediation system for mobile payment". We have enriched some of the platform's functionalities during the technical implementation while keeping the basic functions already presented in the first article. We divided the modeling of the platform into two physical layers:

Layer 1: Figure 3 shows all the cases of uses of the functionalities proposed to the client from a mobile application to exploit the services of the platform.

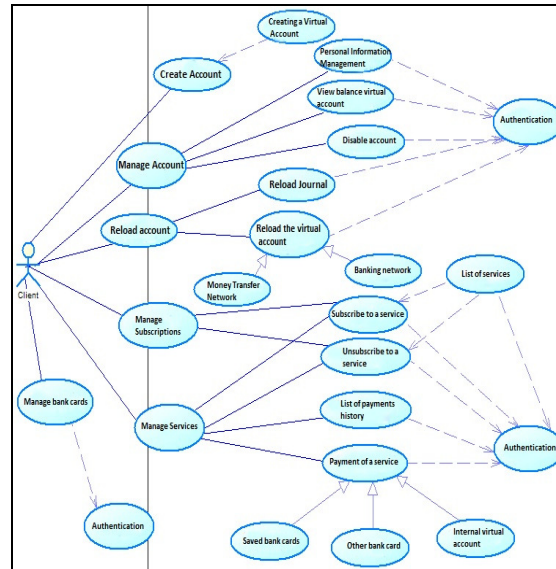


Figure 3: Use cases diagram of use for the Mobile application

The client can use the mobile application to:

- **Creation of a new account:** this function allows the customer to create a new account on the platform, this automatically leads to the creation of a virtual account of the customer balance.
- **Account management:** the customer can modify his personal information via this menu, or to check the balance of his virtual account, or to check the history of his last transactions, and also to disable his account.
- **Configuration of payment channels:** The customer can configure his means of payment via this menu, namely:
 - **Recharging the internal account:** the customer can via a menu to recharge his virtual account via his credit card or through the institutions of money transfers.
 - **Saving credit cards:** The customer can use this menu to save in a secure manner, as many credit cards as he wishes (PAN, DATE EXPIRATION, and CVV).
 - **Mini-statement consultation:** The client can access the mini-statement of his virtual account via this menu.
- **Configuration of the services:** The customer can use this menu to configure his services, the

subscription to a new service requires the identification of the customer with his supplier.

- **Payment of services:** this menu allows the customer to pay his royalties, he has the choice to recover all his royalties or to choose a particular. After the selection of the means of payment (Virtual Account, Credit Card...), the platform automatically takes care of the rest of the operation.

Layer 2: Figure 4 presents the platform administration use cases:

- The management of the customers.
- The management of the services.
- The transactions details consultation.

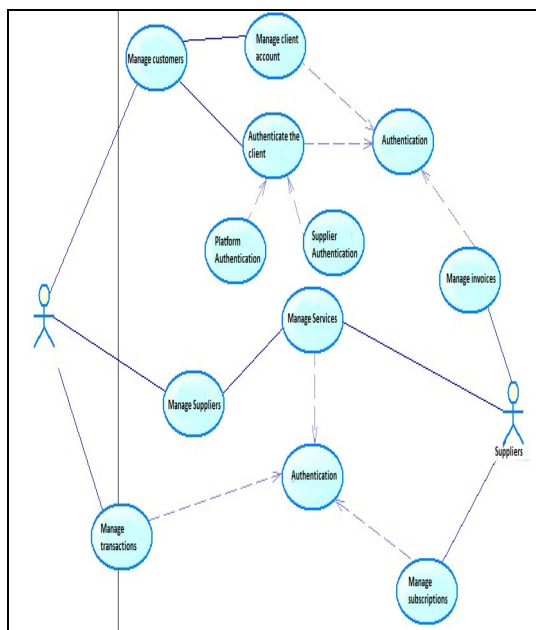


Figure 4: Platform administration use cases

Layer 3: For our simulations, we developed a prototype of application providing Web services similar to those proposed by traditional service providers and who are:

- Client verification.
- List of the royalties.
- Payment of the services.

7. UML SEQUENCE & ACTIVITY DIAGRAM

7.1. Creating a new account :

The client begins with a request to create a new account by entering his email address (Figure 5),

the platform checks if this address is already taken by another user, otherwise the client can complete the other information (First name, Name ,Address), after validation, the platform also retrieves the telephone number and the telephone IMEI, this information will be used in case of theft of the telephone, it then proceeds to the creation of the user's account, this entails Automatically creating the customer's virtual account, an email is sent to the customer for activation of his account.

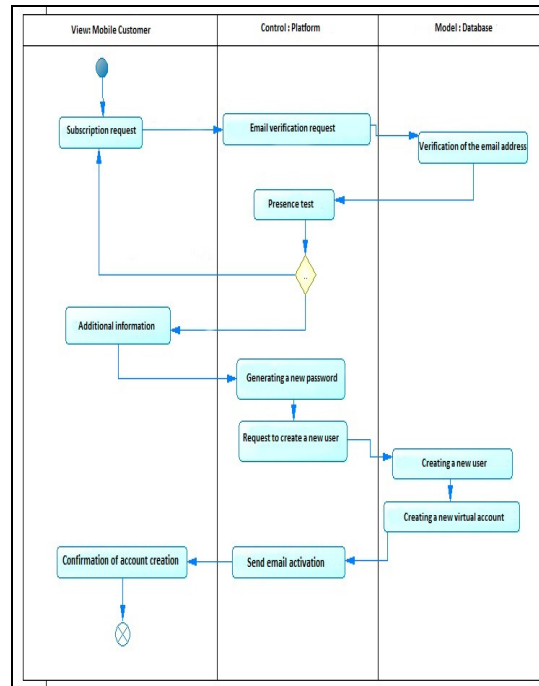


Figure 5: Sequence diagram of the creating a new account.

7.2. Reload Internal account :

The platform offers the customer a virtual account for the payment of his fees, this service is for people who do not have a bank account, or do not wish to use their bank card for security reasons.

The customer can choose between two modes of recharge proposed by the platform (Figure 6):

- **Transfer of money:** The customer enters the identifier received after a transfer of money, the platform recharges the virtual account of the customer after verification of this identifier.
- **Credit card:** The customer can use his bank card to recharge his virtual account.

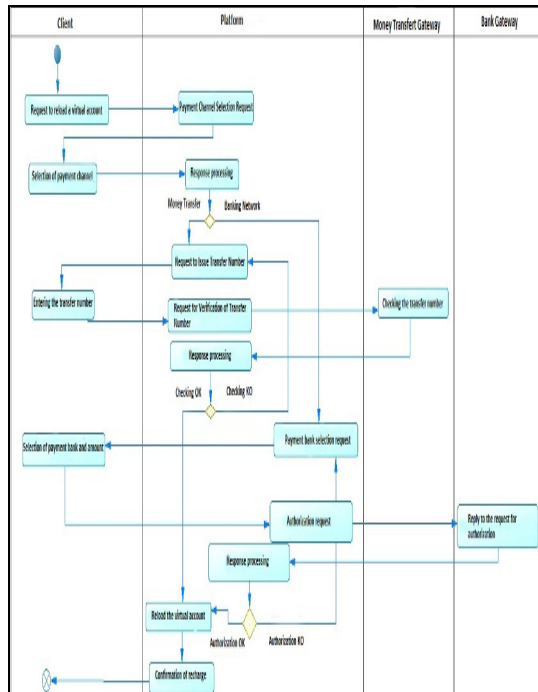


Figure 6: Sequence diagram of the reload of the virtual account

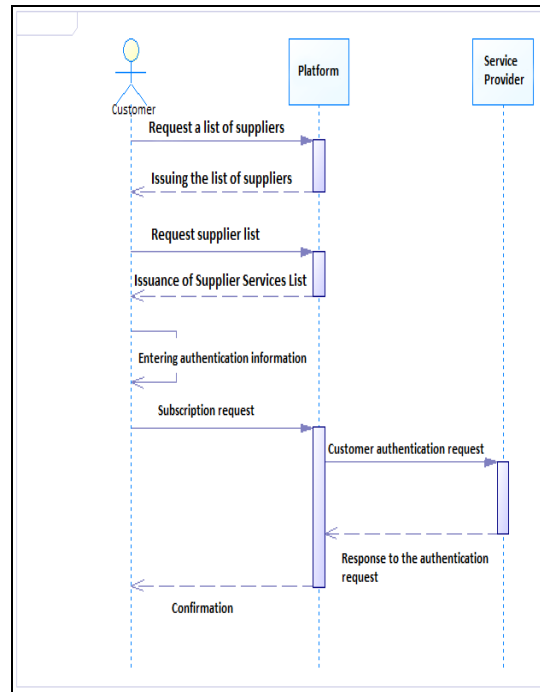


Figure 7: Sequence diagram of the services subscription

The customers can also save its credit cards by a secure way in a platform, so the customer will not need to enter credit card information for each payment transaction, but it is limited only to selecting the desired account for the validation of its payments.

7.3. Subscription to services:

The customer can list the partner suppliers of the platform via a menu and choose the desired service, the customer must identify himself to his suppliers, and after confirmation the customer begins to receive his royalties automatically.

The customer can unsubscribe from a service at any time via another menu.

7.4. Royalties payments:

At the customer's login, the platform automatically recovers all of its royalties in a single menu, the customer can choose between the total payment of all his royalties or choose a particular one (Figure 8). After validation the customer chooses the desired method of payment:

- **Payment by credit card:** the platform sends a request for payment authorization to the customer's bank via interbank networks (VISA, MASTERCARD ...).
- **Payment by internal virtual account:** the platform debits the client's internal virtual account.

The platform ensures the payment of the customer's royalties from its suppliers, and guarantees the compensation based on the daily transaction log.

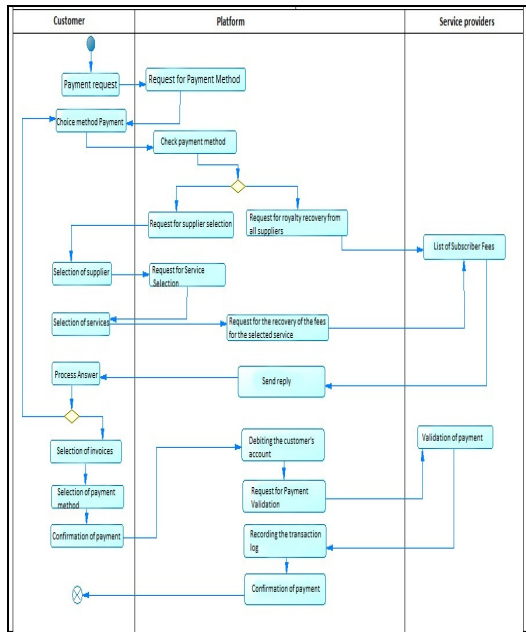


Figure 7: Activity diagram of the royalties' payment

8. TECHNICAL IMPLEMENTATION

The proposed solution allows the customer via a mobile application to exploit the services of several providers through a central mediation platform (Figure 9). Each vendor has a different exchange format, the platform must be able to interact with all of these formats in a transparent way to the client.

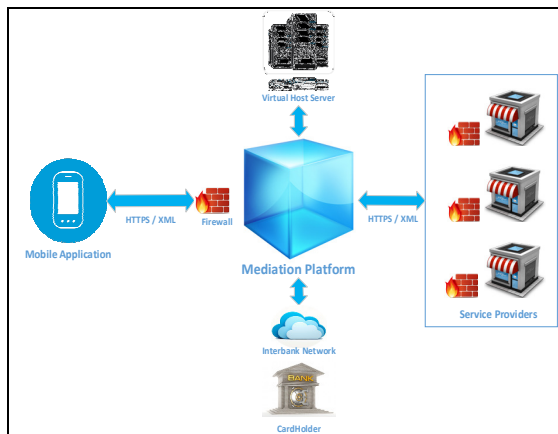


Figure 9: Global description of the mediation platform

Thus, we have divided our architecture into four different layers (Figure 10):

- **The mobile client (Layer 1):**

We chose the Android technology for the development of the mobile application, we used the KSOAP2 library to call the web services of the platform. It is a free library allowing the

implementation of the SOAP protocol under Android [5].

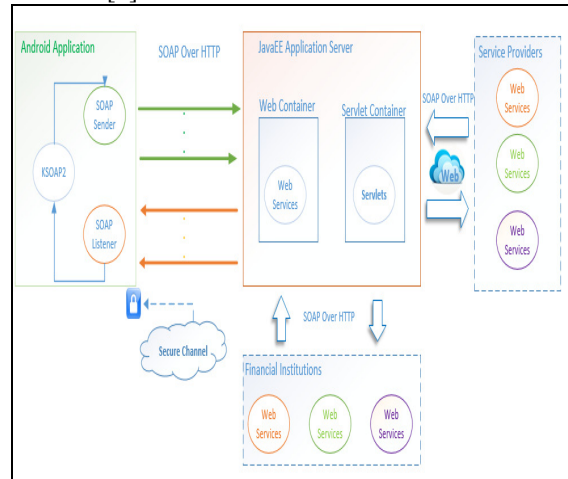


Figure 10: Flows of interaction between the components of the platform

Android offers a class called **AsyncTask** for asynchronous processing, as its name suggests, without needing to manipulate Threads and Handler [6], in our case the call to web services, it has four main methods, including Method **onPreExecute** (for processing initialization), the **onProgressUpdate** method (for processing status), the **onPostExecute** method (for retrieving the processing result), and the **doInBackground** method that performs the requested processing. In this method we call on web:

```
protected String doInBackground(String... args) {
    String response = null;
    final String NAMESPACE =
        "http://ws.PlateformeMpay.com";
    final String URL =
        Var_IP_ADR+"/Plateforme_Mpay/services/Authentication
        ?wsdl";
    final String SOAP_ACTION =
        "http://ws.PlateformeMpay.com";
    final String METHOD_NAME = "authUsers";

    try{
        SoapObject request = new SoapObject(NAMESPACE,
        METHOD_NAME);
        // Add properties
        request.addProperty("email",args[1]);
        request.addProperty("password",args[2]);
        // Create a new envelope object
        SoapSerializationEnvelope envelope = new
        SoapSerializationEnvelope(SoapEnvelope.VER11);
        envelope.setOutputSoapObject(request);
        HttpTransportSE ht = new HttpTransportSE(URL);
        ht.call(SOAP_ACTION, envelope);
        SoapPrimitive responseSoap =
        (SoapPrimitive)envelope.getResponse();
        response = responseSoap.toString();
    } catch (Exception e) {
        e.printStackTrace();
    }
    return response;
}
```

- **The central platform (Layer 2):**

The implementation of the central platform is done under the JEE technology while respecting the MVC pattern, we have deployed the platform in the Tomcat application server, we have generated the web services thanks to the Axis2 SOAP engine [4].

- **The service providers (Layer 3):**

In our experiment, we simulated services offered by different suppliers (Water, Electricity, Telephony), via Web services similar to those in reality:

- Client identification.
- List the royalties of a client.
- Payment of a client royalties.

- **The financial institutions (Layer 4) :**

This layer covers the various channels of communication with all financial institutions (banks, money transfer organization ...) thus enabling the client to:

- Reload the virtual account via the banking networks.
- Reload the virtual account through money transfer agencies.
- Save the client credit cards in a secure way on the platform.
- Payment of fees via interbank networks.
- Payment of fees through its virtual account.

Also, an interface allowing the customer to exploit the balance of his virtual account for E-commerce payments.

9. THREE-FACTOR AUTHENTICATION

Despite their well-known security issues, passwords are still the most popular method of user authentication. It is always possible to guess the passwords of the users thanks to attacks based on the dictionaries of the passwords generated because of their limited entropy [10].

The FIDO standard defines the various references in terms of good authentication practices [11], it requires, for strong authentication of a system, the implementation of three means of authentication, otherwise, at least two means in case. This includes something you know, something you have and something you are [12].

9.1. Something you know: PASSWORD

As the first level of security, the platform requires an Email / Password for client

authentication (Figure 14), the e-mail address of the client is verified at the time of creation of the account. For a higher level of security, the platform also recovers the IMEI and the customer's telephone number, thanks to both information the customer can limit access to his account only from his own smartphone and his SIM card.

9.2. Something you have: NFC Card

The NFC (Near Field Communication) stands for RFID-derived contactless technology, first developed by Sony and Phillips and subsequently by Nokia, Samsung, Microsoft and others [7].

This technology allows the exchange of data at short distance and will be implemented in short term in areas as diverse as:

- Contactless payment from a mobile phone or credit card,
- Access control (company badges, car keys, ticketing, transport cards ...)
- Couponing (coupons or loyalty cards ...).

We used this technology as a physical means of authentication using NFC cards (Figure 11), which the client can set from his smartphone: The platform generates a new identifier for the client, which will be transmitted to the client's smartphone via A web services, the mobile application proceeds to write this identifier as soon as the client approaches a new NFC card of the smartphone.



Figure 11: Example of a 125 kHz MIFARE Classic card.

For the implementation of NFC technology, Google has set up ready-to-use libraries in three modes [8]:

1. Read / Write Mode: Allows the NFC device to read and / or write on NFC sticky and passive tags.

2. P2P mode: allowing the NFC to exchange data with other NFC peers, this mode of operation is used by Android Beam.

3. Host Card Emulation (HCE) mode: allowing the NFC device itself to act as an NFC

card. The emulated NFC card can then be accessed by an external NFC reader, such as an NFC point of sale terminal.

In our case, and in a first step, we will exploit the first write mode on NFC tags, the (Figure 12) illustrates the mechanism of management of NFC tags at the level of the Android system. Usually the phone begins with the detection of a new NFC TAG, although the NFC option must be activated on the phone and it is unlocked, to discover a new NFC tag, the system automatically loads itself By extracting the URI or MIME containing the data by putting it in an Intent, that said that there are several NFC standards, in general Android supports the NDEF format "NFC Data Exchange Format" [9], otherwise, Android offers the `android.nfc.tech` library for communication with other protocols or to create its own protocol.

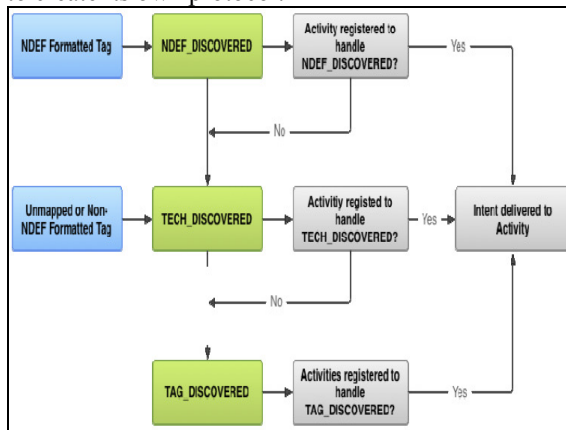


Figure 12: NFC tags management mechanism at the Android system level.

In NDEF format, the data is encapsulated in a message called **NdefMessage**, each **NdefMessage** message is composed of several **NdefRecord** (Figure 13), and the **NdefRecord** Header contains a TYPE field consisting of two elements:

- **TNF (Type-Name-Format):** A 3-bit field that indicates how the "Type" is interpreted.
- **The Data Type.**

On detection of a new NFC Tag, the system retrieves these two fields in a first place, and according to this information encapsulates the data by priority in one of the three **Intent** (Figure 11):

- ACTION_NDEF_DISCOVERED
- ACTION_TECH_DISCOVERED
- ACTION_TAG_DISCOVERED

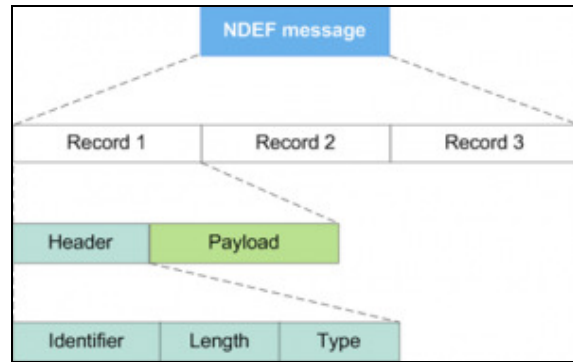


Figure 13: NFC Data Exchange Format (NDEF)

In the first place, Android begins by searching for activity that filters on the `ACTION_NDEF_DISCOVERED` Intent, this activity will have the highest priority, when the system does not find any activity that handles this type of Intent so it tries to start The activities of second priority whose type of Intent is `ACTION_TECH_DISCOVERED`, if no activity answers then it goes to the activities of last level whose type of Intent is `ACTION_TAG_DISCOVERED`, otherwise the telephone does not react.

9.3. Something you are: fingerprint

One of the most widely deployed biometric techniques is digital fingerprint detection technology. It is widely used in various industry sectors such as defense, healthcare, commercial, and mobile applications, among others. It helps to provide practical security solutions that eliminate the need for passwords [14]. Recently, several mobile device manufacturers are beginning to integrate the fingerprint sensor on their smartphones, including Apple and Samsung, according to a study, 50% of deliveries of smartphones will have a fingerprint sensor in 2019 [15]. Samsung makes available an API called Pass SDK [13], allowing developers to introduce fingerprint recognition into their applications.

On our part we have used this technology as a third factor of security (something you are), for the validation of the customer's fingerprint payments.

This library offers a class called **PassActivity** which allows to parameter several variables (Example: the number of fingerprints recorded on the Smartphone ...).

The **PassActivity** class has several "Listener" to check whether the fingerprint is saved, thus authentication succeeded or not, thanks to the variable

STATUS_AUTHENTICATION_SUCCESS in the **SpassFingerPrint** class. Before any processing, the system checks whether the smartphone supports fingerprint reading (SAMSUNG Galaxy S5 minimum required), if so, the user has the ability to:

- Identification of the fingerprint.
- Registration of the fingerprint (Maximum 3 fingerprints).
- Removal of a fingerprint.
- ...
-

10. REALIZATION

The choice of technologies was justified in our first article, ideally it is advisable to use hybrid technologies for the development of mobile applications to cover all mobile OS (Android, iOS, Rim ...). Hybrid technologies (Ionics, Cordova, SenchaTouch ...) are increasingly effective and can also interact with certain smartphone sensors, except that we have found that they still have limits on certain sensors, especially the NFC sensor, Fingerprint, which is why we chose Android.

10.1. Login menu

Figure 14 shows the login menu of the application, the client can either enter its Login / Password, or use NFC card for authentication.

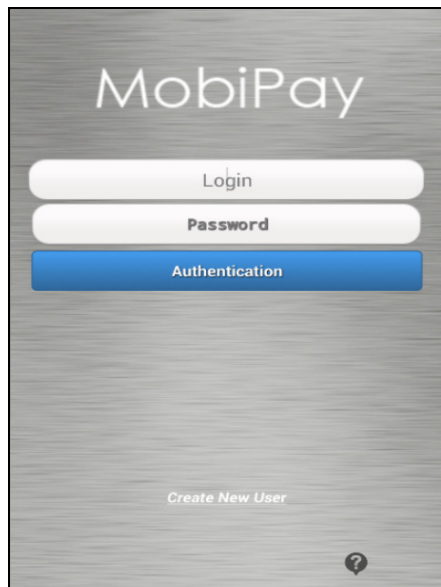


Figure 14: Login user menu

10.2. Creating a new account

To create a new account, the client starts by entering his email address (figure 15).



Figure 15: Creating a new account menu 1

The platform checks if this address is not already taken by another user, otherwise the client can complete his personal information (Figure 16).



Figure 16: Creating a new account menu 2

The application automatically retrieves the phone number and IMEI of the smartphone. After validation, the temporary password is sent directly to its mailbox, which the client must modify at the first connection (Figure 17).



Figure 17: Creating a new account menu 3

10.3. Main menu

After login, the client directly accesses the main menu of the mobile application (Figure 18)



Figure 18: Main Menu

From this menu the customer can:

- Reload the virtual account.
- Configuring services.
- Payment of royalties.
- Account configuration.

10.4. Reload the virtual account

This menu allows the customer to recharge the balance of his virtual account thanks to the different payment channels (Figure 19).



Figure 19: Electronic payment channels

10.5. Services configuration

This menu allows the configuration of the supplier services (Figure 20).



Figure 20: Services configuration Menu

The customer must enter his credentials for each service (Figure 21).

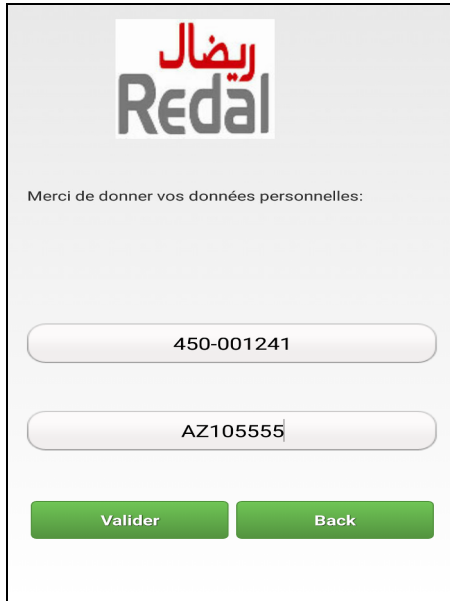


Figure 21: Example of customer identification

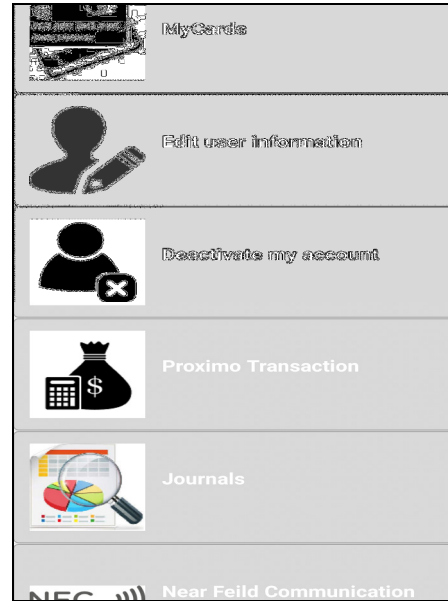


Figure 23: Client account setup menu

The customer can also unsubscribe from a service via another menu (Figure 22)

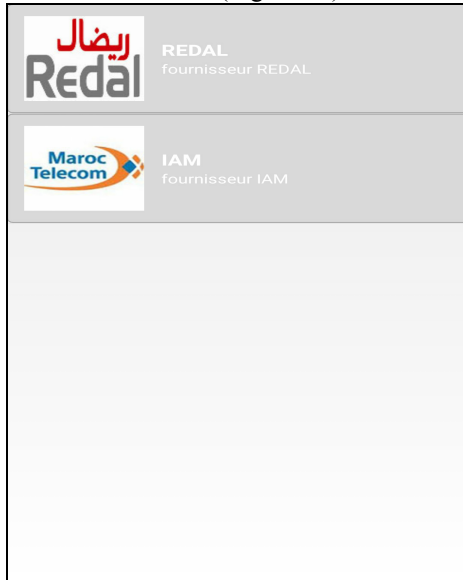


Figure 22: Unsubscribe from services Menu

10.6. Client account configuration

This menu (Figure 23) allows the customer to:

- The configuration of a new NFC card.
- Deactivation of his account.
- Consultation of the mini statement.
- Modification of personal information.
- Saving credit cards.

10.7. Saving Client's credit cards

This menu allows the customer to save as many credit cards as he wants (figure 24).

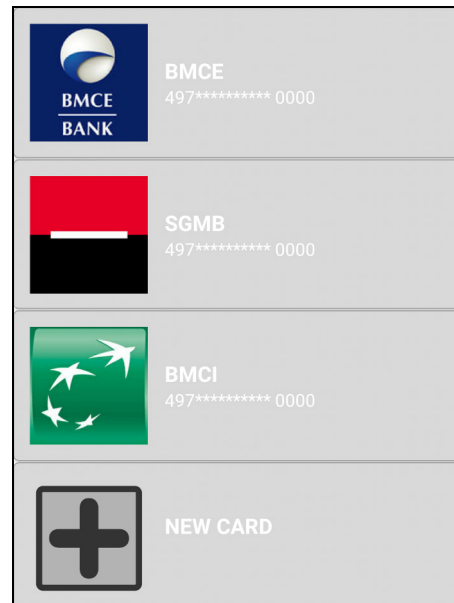


Figure 24: Client credit card menu

At the time of payment the customer has only to choose the bank card that he wishes and the payment is done automatically.

10.8. Payment of royalties

This menu allows the customer to pay his royalties (Figure 25), he has the choice between the

recovery of all his royalties, if not to choose a particular.

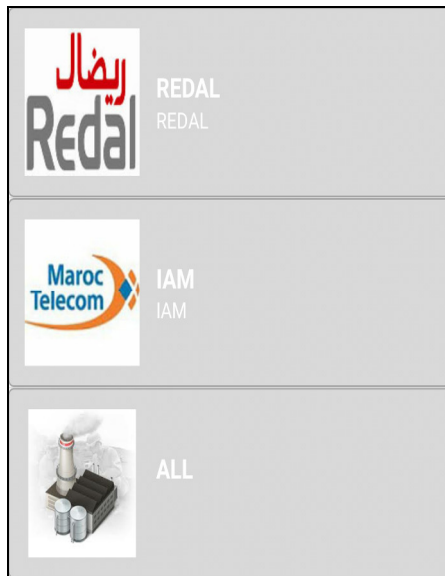


Figure 25: Customer Royalty Payment Menu

After selecting the desired invoices, the customer chooses the desired means of payment via another menu (Figure 26), namely:

- **Virtual account:** Payment by the balance of the internal virtual account.
- **Saved credit card:** the customer chooses the payment by the selection of one of the credit cards already registered in the platform.
- **Other credit card:** the customer can use a credit card not registered in the platform.

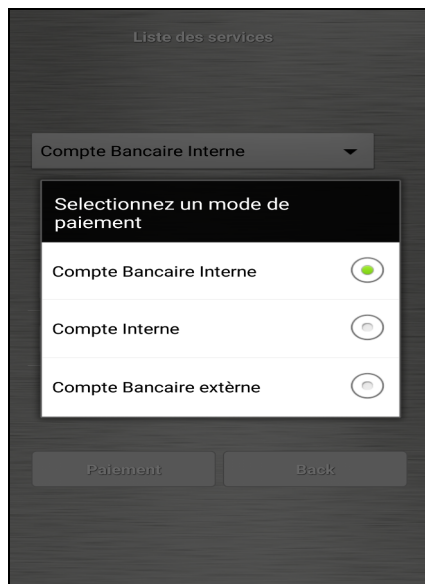


Figure 26: Customer Payment Menu

11. RESULTS AND PERSPECTIVES

In the first architecture (Figure 10), the platform offers several web services called by the mobile application, if a malicious user manages to recover the source code of the application, which is possible on Android, it can easily Attack these different web services.

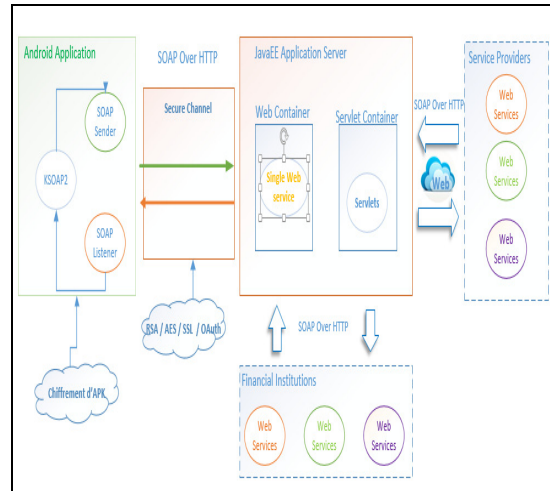


Figure 27: Proposed new architecture of the platform

To solve this problem, we thought of the implementation of an architecture based on a single web service (Single Web Service). This web service has a controlling role, it receives the customer's requests and triggers the appropriate action. In this model it will be easy to set up an intelligent agent to detect any suspect behavior of the client. Also, the advantage of using a single communication channel facilitates the implementation of a more secure encryption protocol, in particular AES and RSA

On the other hand, the current model requires us to develop a communication interface for each supplier, which is why we have limited ourselves to the payment of invoices, so it would be interesting to set up a layer based on the notions of the semantic web to automatically recognize the web services offered by the providers.

12. CONCLUSION & FUTURE WORK

Thanks to this study, we concluded that it is possible to set up a mobile payment ecosystem capable of conquering traditional payment solutions (ATM, POS ...). In this level, the use of NFC technology has been limited only as a means of authentication, but we have found that it is possible to extend our platform to a NFC payment solution, of this kind of platform remains very varied...

REFERENCES:

- [1] "A Secure Mobile Electronic Payment Architecture Platform for Wireless Mobile Networks", Phone Lin, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 7, JULY 2008.
- [2] "A User Friendly Transaction Model of Mobile Payment with reference to Mobile Banking in India", Vibha Kaw Raina, International Journal of Information Technology, Vol. 18 No. 2 2012
- [3] <http://fr.wikipedia.org/wiki/Micropaiement>
- [4] <https://axis.apache.org/axis/java/index.html>
- [5] "A light Mobile Web Service Framework based on Axis2", Zhun Shen, Ka Lok Man, Hai-Ning Liang, Nan Zhang, Charles Fleming, David Olalekan Afolabi, Yanyan Wu and Sheung-Hung Poon, Future Information Communication Technology and Applications: ICFICE 2013
- [6] <http://developer.android.com/reference/android/os/AsyncTask.html>
- [7] "NFC (Near Field Communication): Principes et applications de la communication en champ proche", Dominique Paret, Xavier Boutonnier, Youssef Houiti, Dunod, 4 juil. 2012
- [8] "Beginning NFC: Near Field Communication with Arduino, Android, and PhoneGap", Tom Igoe, Don Coleman, Brian Jepson, O'Reilly Media, 2014.
- [9] "Professional NFC Application Development for Android", Vedat Coskun, Kerem Ok, Busra Ozdenizci, John Wiley & Sons, 3 avr. 2013 - 312 pages
- [10] "A Comparative Usability Study of Two-Factor Authentication", Emiliano De Cristofaro, Honglu Du PARC, Julien Freudiger PARC, Greg Norcie, Network and Distributed System Security (NDSS) Symposium, Jan 2014
- [11] "FIDO Security Reference", FIDO Alliance Proposed Standard, 8 Dec 2014
- [12] "Three-Factor Authentication for Automated Teller Machine System", Jane Ngozi Oruh, Michael Okpara, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.6, December 2014
- [13] <http://developer.samsung.com/resources/pass>
- [14] "Fingerprint Sensors Market by Type (Swipe & Area), Technology, Material (Optical Prism, Piezoelectric, Capacitive & Adhesives), Application (Mobile, Government, Healthcare, Commercial Security & Others) & Geography - Global Forecast to 2014 - 2020", marketsandmarkets.com, June 2015.
- [15] "Fingerprints On Mobile Devices: Abusing and Leaking", Yulong Zhang, Zhaofeng Chen, Hui Xue, and Tao Wei, FireEye Labs.
- [16] E.W.T. Ngai, A. Gunasekaran, July 2005, "A review for mobile commerce research and applications", International Journal of Business Innovation and Research.
- [17] Jerry Gao, Krishnaveni Edunuru, Jacky Cai, and Simon Shim, IEEE International Workshop on Mobile Commerce and Services (WMCS'05), "P2P-Paid: A Peer-to-Peer Wireless Payment System".
- [18] Ashutosh Saxena, Manik Lal, Das Anurag Gupta, IEEE International Conference on Mobile Business (ICMB'05) "MMPS: A Versatile Mobile-to-Mobile Payment System".