International Journal of Wireless Communications and Mobile Computing
2021; 9(1): 1-6
http://www.sciencepublishinggroup.com/j/wcmc
doi: 10.11648/j.wcmc.20210901.11
ISSN: 2330-1007 (Print); ISSN: 2330-1015 (Online)

Using USSD-based Mobile Payment in Context of Low Internet Connection

Paul Dayang*, Abassi Hamza

Department of Mathematics and Computer Science, Faculty of Science, The University of Ngaoundere, Ngaoundere, Cameroun

Email address:

pdayang@univ-ndere.cm (P. Dayang), hamzaabassi14avril@gmail.com (A. Hamza)

*Corresponding author

To cite this article:

Paul Dayang, Abassi Hamza. Using USSD-based Mobile Payment in Context of Low Internet Connection. *International Journal of Wireless Communications and Mobile Computing*. Vol. 9, No. 1, 2021, pp. 1-6. doi: 10.11648/j.wcmc.20210901.11

Received: July 7, 2021; **Accepted**: July 19, 2021; **Published**: September 29, 2021

Abstract: With the evolution of mobile technology and the emergence of new devices called "smartphones", a new payment method called "mobile payment" has emerged. Smartphones occupy our daily life, so much so that some people do not imagine their routine life without them. If smartphones occupy the daily life in some African countries, orange money or MTN mobile money known as mobile payment accounts are even more. In Cameroon the mobile accounts (orange money or MTN mobile money) are so important that their use has become almost inevitable. We meet several utilities of these payment methods, we may cite electricity bills, purchase of products and services, payment of school and university fees etc. But this model of payment presents some limits among which we have the problem of ergonomic, proof of a payment and so on. In this work, we offer a secure, simple and powerful mobile payment model for both online using Internet as well as offline using Unstructured Supplementary Service Data (USSD). The payment model must be accessible to all, easy to use and shall support online or offline system. Inspired by the mode of operation of orange money outlets, this model uses two SIM cards, one commercial (seller) and the standard one (buyer). After designing an easy interface composed of two compulsory fields (phone number and amount), a USSD code is executed internally in our system requesting a withdrawal on the customer number. After the confirmation from the customer, the money is transferred to the seller's account. The model does not use of save any confidential information neither for the seller nor for the buyer.

Keywords: Mobile Payment, USSD, AT Command, SIM, Security

1. Introduction

The rate of banking services in the sub-Saharan African countries is estimated at 10% unlike developed countries like USA where the rate is 90% [1]. Since 2015, this rate has increased considerably, so Cameroon is moving to a rate of 20%. Therefore, we noticed an insufficiency linked to banking services compared to countries which are economically at the same level. In fact, every business activity in order to grow and to prosper needs to deal with financial transactions that should be not only easy to process but also secured. Another challenge we are facing is the low Internet connection which leads to poor online services including online payment.

Since 2012, the two leaders in mobile, MTN and Orange Cameroun, have launched the activities of mobile money transactions [2]. In Cameroon, the launching of mobile money has led to several payment methods. Thus, we have online payment APIs, payment methods via operators and many more. But until then, there is a lack of a payment method in a local network of an enterprise and small shops around a corner of street. In addition, the interfaces of the existing methods are not ergonomic enough.

Therefore, we propose a payment model that will process payments both in a local network and online as well. A secure, reliable and powerful payment model and available to all. The proposed model must meet the constraints of non-repudiation, confidentiality, integrity and authentication. The payment approach is simplified, so that each person possessing an Orange Money or MTN mobile money account, must be able to proceed transactions via a user-friendly interface.

In order to implement the proposed model, we used a Huawei model E303 modem and a commercial Orange SIM to which we send "AT commands" via a serial port developed in

PHP programming language. Thanks to existing technical ingredients and tools, we have been able to implement our model considering security and integrity constraints linked to such important transaction activities.

This paper is organized as follows: The first part scrutinizes the generalities on existing payment models, the second part deals essentially with the online payment methods existing in Cameroon. The next part describes the suggested architecture including the tools that were used for its implementation. In the fifth part, we discuss the results reached and show how the suggested model takes the security constraints into consideration. The paper ends with a general conclusion and perspectives.

2. Generalities on Payment Models

Mobile payment is defined as the use of mobile devices, such as mobile phones to initiate payment transactions [3]. Several payment models exist. A popular payment model is the one base on SMS as transport channel which sends transactions to payer as SMS message to be confirmed (yes/no) [4]. The advent of mobile accounts has also spawned several payment-based businesses using mobile accounts. This is the case in Cameroon, where several APIs have been created. The APIs allow merchant sites to receive mobile payment via mobile accounts on its site.

2.1. Mobile Payment Models

A non-exhaustive list of payment models is as follows:

1) The bank-centred model: the bank is the main actor using this model. It manages the entire transaction and distributes the property rights [5].
2) The third-party model: an actor other than a bank or a mobile actor has the management of the payment service. Some agents have opportunities to position themselves in this market, such as providers of electronic payment services that already have experience in the mobile or financial environment [5].
3) The collaboration model: as the name implies, it is a collaboration between financial intermediaries and mobile operators. Together they share the responsibility for the service as well as the sources of income.
4) Complementary money: it is not an economic model strictly speaking, but a formula leading to the development of "local" complementary currencies. Mobile payments are then not based on a currency recognized by central banks, but by a complementary private currency whose development has a commercial vocation. These payments are originally assimilated to the use of vouchers distributed free of charge by partners of the service recipient or by itself.

2.2. Mobile Payment Technologies

The evolution of mobile technology is left from a simple communication tool to a computer in the pocket, so several applications have been developed and several technologies have emerged among which we have mobile payment technologies. In order to continue to use mobile technology to better meet the daily needs of a user, several attempts have been made to provide a phone with a financial management system to replace the conventional physical wallet [6]. Thus, as mobile payment technologies, we have among others:

1) Mobile Wallet: The mobile wallet application can have the same composition as a traditional wallet, which can hold payment cards, membership cards, transport cards and loyalty cards [6].
2) Near Field Communication (NFC): NFC is a short-range, high-frequency technology that enables contactless transactions and the exchange of messages between two devices at a distance of a few centimeters. NFC devices can operate in three modes: drive / recorder (an active device communicates with a passive device), peer-to-peer (active devices communicate with passive or active devices), and optional card emulation modes [7].
3) Short Message Service (SMS): SMS is a mobile phone service that can transmit short text messages. SMS is a smart service because it can store messages when the target mobile device is turned off and transmits messages when the device is used again. Basically, any information that comes in a short text message can be delivered via SMS [8].
4) Unstructured Supplementary Service Data (USSD): USSD technology is a feature of mobile devices to trigger a service after sending an SMSC (a kind of SMS signalling, free). Unlike SMS, data is not stored and can only be accessed when logging in. The USSD is mainly used in areas of the world where populations are poorly banked and where the mobile is also a management tool for transactions such as money transfer, bill payment, prepaid card recharge, account tracking. The USSD remains the preferred communication channel for the development of services [9].
5) Wireless Application Protocol (WAP): WAP is a technology that provides a mechanism to display Internet information on a mobile phone or other wireless device. This is done by translating information from the Internet into a format that can be displayed in the constraints of a mobile device. In addition, setting up a WAP phone for new WAP services is problematic. Some twenty different parameters are needed to access the WAP service, which can discourage users [8].
6) Radio-frequency identification (RFID): RFID is similar to the NFC in that it uses radio waves to communicate transaction information [10], but it allows the exchange of data over longer distances (up to several meters). As with NFC technology, it requires an RFID chip (or tag) to be embedded in the user's phone and can be used for both cash and peer-to-peer transactions.
7) Quick Response (QR) CODE: QR Code is a two-dimensional barcode containing the consumer's payment account information, which is then scanned at the checkout by the merchant's device. The user's

account is associated with a payment account, to which the amount of the transaction is automatically billed [9].

8) Bluetooth Low Energy (BLE): BLE is a wireless transmission technique. Compared to Bluetooth, the BLE allows a flow of the same order of magnitude (1 Mb / s) for a power consumption 10 times less. But Bluetooth has some inherent advantages that can make it a serious competitor. Bluetooth runs a much larger distance than NFC, which allows for transactions from anywhere in the store rather than forcing customers to queue for a fixed terminal [9].
9) BlockChain: A blockchain is a distributed database whose information, sent by users, is checked and grouped at regular time intervals into blocks, bound and secured through the use of cryptography, and thus forming a chain. It is this technology that allows the "trust" to be established between different agents of the system, chosen by the fintech WeCashUp which offers African e-merchants "a unique interface" allowing them to integrate all the solutions from Mobile Money [9].

3. Online Payment Methods in Cameroon

The possibility to a subscriber to have a mobile account with his number has led Cameroonians to turn to another means of payment, so payment by Orange money or MTN mobile money is used in almost all areas: payment of fees. education, payment of bills, payment of fuel, payment of telephone credits etc. Investors becoming aware of the magnitude that is taking mobile accounts have seen a possibility of online payment via a mobile account (Orange money or MTN mobile money).

Thus, several APIs have emerged in Cameroon in particular and Africa in general.

1) AByster: An API providing components to manage calls from a mobile application, a website or web application to the payment platform. All communications between the two entities are asynchronous via a RestFull API. AByster provided 02 environments for the use of its services [11].
2) WeCashUp: An API with several means of payment (Cash, Mobile Money, M-wallet, Card and Crypto). At WeCashUp as well as at AByster we also have two environments namely the production environment and the test environment. Using HTTPS for secure communication wecashup realizes a two-step transaction.
3) Monetbil: An API with three payment methods (Orange Money, MTN mobile money, express mobile union) Monetbil is a payment method for digital goods and services online using the billing service of mobile operators. Monetbil offer e-merchants a simple, fast and secure mobile phone payment method. And contributes to the significant increase in their turnover. There is no subscription at monetbil, just cut 3% on transactions [12].
4) VuSur: VuSur is simply an intermediary unit. The purchase with VuSur takes place in four stages: Visit a commercial site, send the links of the desired articles, set the order and receive the article [13].
5) PayPal: PayPal Cameroon is an online payment service that allows you to make purchases, receive payments, or send and receive money around the world. Before you can do any transaction on PayPal you must first have a PayPal account. To create a PayPal account, simply go to PayPal Cameroon and fill in the requested information.
6) Visa or MasterCard Money Transfer: Also known as credit card payment mode, there are different kinds of Visa or MasterCard cards marketed by diverse credit institutions.

In general, we are facing the challenge of low Internet connection which leads to poor online services including online payments. Therefore, looking for additional and secured payment methods is necessary.

4. Implementation of an Approach Based on USSD

The suggested approached is an online and offline payment model. The architecture is proposed followed by its implementation and test in real environment.

In the suggested architecture (Figure 1), we distinguish between human actions and those of mobile terminals. Thus, we see the orders placed from the interfaces of the mobile terminals and the encrypted commands that will cross the GSM network [14]. Indeed, we are aware of the fact that the information is encrypted using an encryption key contained in the SIM card [15].

The whole architecture as shown in Figure 1 is described as follows:

1) Sending a number: the customer starts by giving the number to the salesman it is the first action in this process;
2) USSD query payment: the seller executes a USSD query on the mobile with the customer number and transaction amount;
3) USSD CODE: The USSD code travels in a secure channel to the platform (USSD Gateway);
4) Request confirmation: the platform sends a confirmation request to the customer;
5) Massage request confirmation: the customer receives a confirmation request message telling him which USSD to enter for validation;
6) USSD confirmation with secret code: the customer enters the validation code with the secret code;
7) USSD confirmation: the confirmation USSD travels in an encrypted channel up to platform level;
8) Success: After having debited the account, the platform sends a message of success to the seller;
9) SMS confirmation debit: the seller receives a confirmation of debit message in the customer's account;
10) Payment: the seller after receiving a confirmation message, pays the customer and it is the end of the transaction.

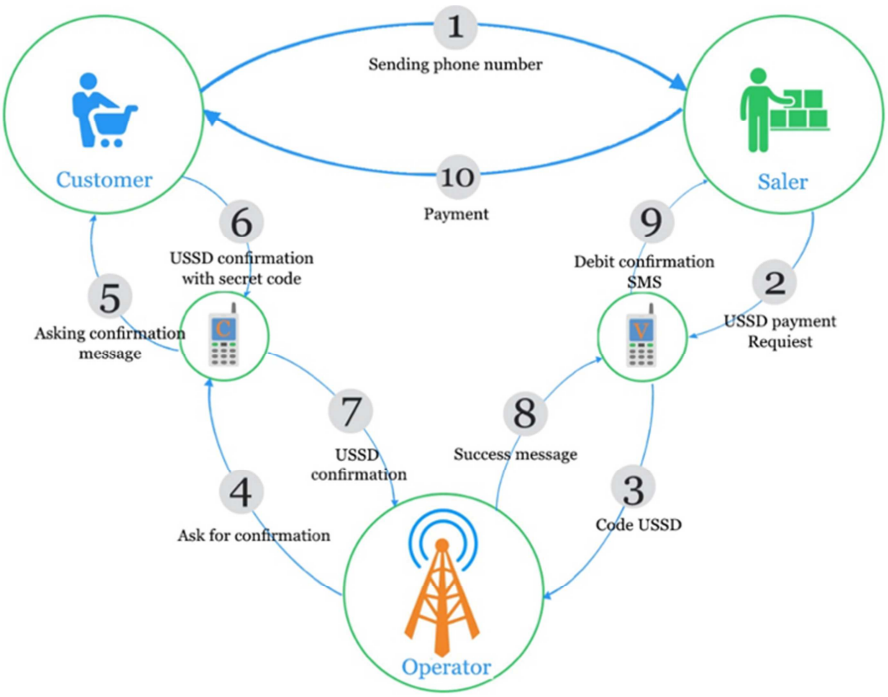

Figure 1. *Architecture based on USSD.*

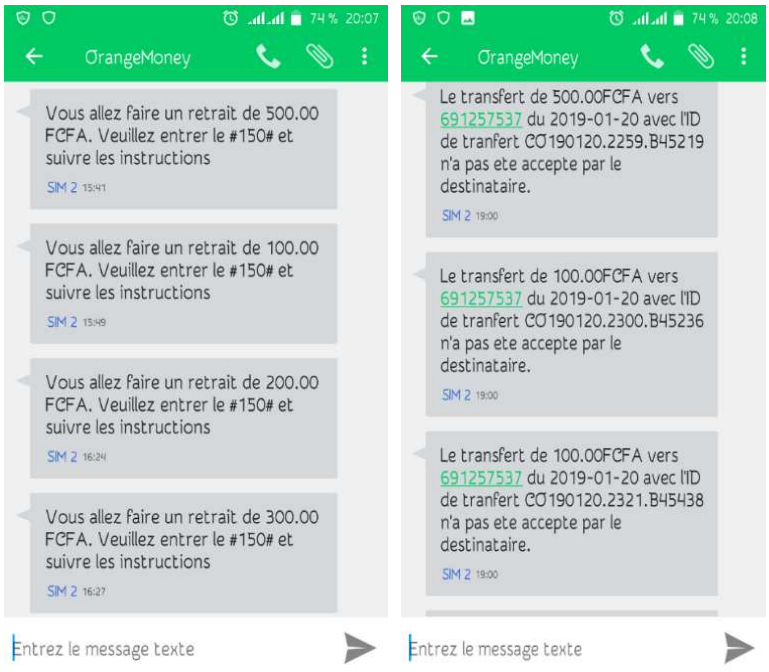

Figure 2. *Payment confirmation messages.*

The prerequisites of the suggested model are a commercial SIM card, then an electronic module that supports ATCommands (a modem, or other ATCommands equipment), a computer, and finally at least one customer with an Orange Money or MTN mobile money account.

Since the model can be used offline, it is possible to implement the proposed model in an intranet and small shops. The proposed model uses the GSM network for transactions. Since all the security measures are put in place by the operator to allow a good transaction, we rely on this security to make our payments online or offline. Nevertheless, for the communication with the payment server, one will need some measure of security.

The system we have put in place is a multi-user system, so it is necessary to make it accessible to different users simultaneously. The implemented application is a web-based system which operates in client-server mode in an intranet or Internet environment. To implement and run the system, we needed several hardware and software tools.

Table 1. *Needed tools.*

Tools	Description
Laragon	A portable, isolated, fast and powerful universal development environment for PHP, Node.js, Python, Java, Go, Ruby.
Laravel	is a free, open-source PHP Web Framework, created by Taylor Otwell for the development of Web applications based on Symfony-based model-view-controller (MVC)
Mobile Partner	A Huawei's generic program for managing USB modem connections

Three payment have been initiated and conducted successfully according ot the Phone payment confirmation message in Figure 2.

5. Conformity to Security Standards

Security is the most important aspect in the field of m-commerce in general and m-payment in particular because, without secure commercial exchange of information and secure financial transactions, no one will trust m-commerce. As a result, various security procedures and mobile payment methods have been proposed and applied to mobile commerce [16]. A secure mobile payment system must have certain properties. It will therefore be a question of whether our proposed system respects these constraints. In this chapter, we will first look at the security aspect of our proposed model, then the limitations of our payment system.

5.1. Confidentiality

The GSM channel is encrypted by the algorithm A5 using a 64-bit key generated from an algorithm stored in the SIM card namely A8. To generate the key Kc from the algorithm A8 a key Ki stored in the SIM card is used. To ensure the confidentiality of the subscriber identity, a Temporary Mobile Subscriber Identity (TMSI) is used. The TMSI is sent to the mobile station once the authentication and encryption procedures have been completed. The mobile station responds by confirming receipt of the TMSI [17].

5.2. Authentication

The authentication protocol used in GSM networks is based on a symmetric crypto system called A3. The unilateral authentication of the terminal consists for the latter to calculate a message authentication code (MAC) in response to a challenge RAND sent by the operator [18]. The authentication protocol used in third-generation networks allows the operator's terminal and network to mutually authenticate [18]. The following figure shows authentication in a fourth-generation network.

5.3. Integrity

The communication in a GSM network is encrypted by a symmetric algorithm, the encryption key is generated from an algorithm stored in the SIM card, which even the phone can never know. The encryption key used by the generation algorithm is also well protected at the SIM card level. After the authentication a secure channel is created and now the communication is encrypted. By means of knowing the content unless you have an encryption key, it is in this way that the integrity of the data is preserved.

5.4. Authorization

A key Ki is assigned to the user, during the subscription, with the IMSI. It is stored in the subscriber's SIM card and in the AuC which is generally part of the network level. In order to avoid any possibility of reading the key Ki, it is never transmitted neither on the radio interface nor on the network. The authentication center also has an A3 algorithm as well as A8 just like the MS. Before starting any communication, the MS must obtain the RAND and generate the SRES using the A3 algorithm on the RAND with the Ki key. The SRES is compared with that of Auc. If it matches then the user can connect to the network.

5.5. Non-repudiation

The Orange Money and MTN Mobile Money accounts are both protected by a password which only the user will have to know normally. Before any operation on an account, even a consultation of the balance, goes through a pass mode. So, when there is an operation on an account outside the deposit, then the password has been entered and the user has somehow passed the password.

6. Conclusion and Outlook

In this paper, electronic payment in Cameroon has shortcomings, due to the low rate of banking. In 2012, the two leaders of the mobile market launched mobile money. Subsequently several means of payment have emerged. But no way allows payment in a corporate network for small shops.

Therefore, we set the goal of proposing an easy payment model that can work online as well as offline. The model proposed in this work fulfills a good amount of the shortcomings identified including ergonomic issues. Furthermore, the model also meets the main security constraints that a payment system must have: confidentiality, authentication, integrity, authorization and non-repudiation.

However, it would be much interesting to improve the way of executing the operations by integrating other payment modes such PayPal, credit cards or automatic bank transfer which are more or less also based on web technologies.

References

[1] TCHOUASSI, G. e. (2013). Influence des réformes bancaires et microfinancières sur le taux de bancarisation dans la zone BEAC. Communication aux Vèmes Journées Internationales de la Microfinance, 12.

[2] NGUENA, C. L. (2015). INNOVATION FINANCIERE ET DEVELOPPEMENT DURABLE AU CAMEROUN: Pourquoi le Développement du « Mobile Banking » est-il Important ? Association of African Young Economists, 16.

[3] GAO, J. K. (2009). A 2D barcode-based mobile payment system. Third International Conference on Multimedia and Ubiquitous Engineering. IEEE, 320-329.

[4] HARB, H. F. (2008). SecureSMSPay: secure SMS mobile payment model. 2nd International Conference on. IEEE, 11-17. (Hany Harb; Hassan Farahat; Mohamed Ezz).

[5] Chaix, L. (2013). Le paiement mobile: perspectives économiques, modèles d'affaires et enjeux concurrentiels. Université Nice Sophia Antipolis, 312.

[6] YONGSUNG, K. W. (2014). System and method for managing mobile wallet and its related credentials. U.S. Patent No 8, 843, 125, p. 14.

[7] BADRA, M. e. (2016). A lightweight security protocol for NFC-based mobile payments. Procedia Computer Science, 705-711.

[8] MCKITTERICK, D. e. (2003). State of the art review of mobile payment technology. 2003-24.

[9] Sylla, A. Le Paiement Mobile: Définition et Technologies utilisées, http://www.assasylla.com/2018/04/03/paiement-mobile-definition-technologies-utilisee (September 2020).

[10] Avery Williamson Sr., L.-S. T. (2013). Solutions for RFID Smart Tagged Card Security Vulnerabilities. AASRI Conference on Intelligent Systems and Control, 282 – 287.

[11] Abyster, sandbox-abyster.appspot.com: https://sandbox-abyster.appspot.com/ABOffer/display.do (November 2020).

[12] Monetbil. Paiements en ligne par téléphone portable au Cameroun, https://fr.monetbil.com (August 2020).

[13] VuSur. Achetez à l'étranger, faites-vous livrer au Cameroun - VuSur, https://vusur.com/fr (November 2020).

[14] Chrystel Gaber, M. A. (2013). Réseaux 4G: anticiper la sécurité des systèmes de transactions sur mobile. 8ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR SSI), (p. 10). Mont-de-Marsan, France.

[15] KORKUSUZ, A. (2012). Security in the GSM network. Bogazici University, Electrical-Electronics Engineering Department.

[16] Saleem, e. A. (2007). "Analysis of mobile payment security measures and different standards.". Computer Fraud & Security.

[17] MARGRAVE, D. (1999). GSM Security and Encryption. George Mason University.

[18] KASMI, C. e. (2011). État des lieux de la sécurité des communications cellulaires.