International Journal of Computer Networks and Communications Security

VOL. 4, NO. 4, APRIL 2016, 107–113
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Secured and Centralized Identification System of Subscribers with Mobile Networks: The Case of SENEGAL

SAMBA NDIAYE[1], LANDRY T. YELOME[2], ABDOURAHMANE RAIMY[3], SIDI M. FARSSI[4], SAMUEL OUYA[5]

[1, 2, 3, 4, 5] Cheikh Anta Diop University, Polytechnic High School, Dakar, Senegal

E-mail: [1]techni133@gmail.com, [2]landry.yelome@gmail.com, [3]araimy16@yahoo.fr, [4]farsism@ucad.sn, [5]samuel.ouya@gmail.com

ABSTRACT

Nowadays, with the mobile phone, it is possible to commit several infringements, threat, blackmail, insult, terrorist acts etc. To mitigate these possibilities, the identification of the subscribers is a necessary and obligatory operation. In Senegal, the identification is a matter of national security. For the best regulation of subscribers, we suggest a platform of secured and centralized identification integrating advanced technologies which will on the run put an end to the unregulated sale of chips. The proof of the good realization of our platform of identification was made by the use of a secure and centralized database where terminals can log for operations of identification. This device will make it possible for the competent jurisdictions to have a visibility on the number of subscribers per operator and the total of subscribers on all the national extent of the territory.

Keywords: *Traffic, Cybercrime, Identification Management, Security, Mobile Network.*

1 INTRODUCTION

In Senegal, the sector of mobile telecommunications is characterized by a sustained high growth of the park of subscribers, 14,959,477 lines, with a penetration rate of 104.45% at the last quarter 2015 [1] and a strong demand of new services starting from 1996, date of exploitation of the first mobile telephone network. Three titular operators of 2G and 3G licensee dominate the market of the telecommunication services. It is SONATEL (Orange) SENTEL (Tigo) and SUDATEL (Expresso). Each operator proposes a strategy to have the maximum of subscribers. Promotions multiply. The chips are sold on the run in the street at all the purses like bread ends. In addition, the Senegalese state has just launched an offer of call for the acquisition of the 4G license [2][3]. The number of subscribers increases in an exponential way. A true difficulty of real identification of the subscribers arises then, on the side of operators as well as on the side of the competent authorities. States will also have a visibility on the real subscribers on all the national extent of the territory. It will be able to thus prevail if there is for example an act such as the cybercrime orchestrated by unspecified subscribers.

This paper suggests a secured and centralized architecture at the Regulatory authority where all the relative data with a subscriber are recorded beforehand with a redundancy with the Ministry for interior and a waiter backup at the Data-processing Agency of State (ADIE).

In the continuation of this paper, we will present in section 2, the context and the challenges. In section 3, we will speak about the current situation of identification of subscribers. As in point 4, we will speak about the modeling of the data. As in point 5, it will be a question of the solution suggested by listing the results resulting from simulation. Lastly, the sixth and last section will be booked with the conclusion and the prospects.

.

2 CONTEXT AND CHALLENGES

The world of today is a world of communication and exchange. Due to terrorism, with the cases of swindle and with the fraud bypassing which threaten peace and the international security [4][5], each State must give itself means of supervising

and to control the activity of the telecom operators, in particular control and traffic, the authorized phone-tapping analysis, the identification of subscribers etc. The identification of subscribers meets a need for national sovereignty and makes it possible to have a visibility on the number of chips sold to each subscriber. With this intention, the government of Senegal, following the example of other governments periodically launches operations of identification of subscribers in collaboration with the operators. However, in spite of their high cost, these operations of identification remain without success. It is noted that many users, continue to communicate without being identified that poses a certain number of problems with the competent jurisdictions which must be looked at throughout the process of attribution and use of the chips.

Whereas on this vigilance depends indeed the veracity amongst subscribers by operator and the total on the numbers on all the national extent of the territory.

3 CURRENT SITUATION OF IDENTIFICATION OF THE SUBSCRIBERS

Today force is to note that the state, even being the main actor, intervenes timidly in the current identification process of subscribers, framed by the decree 2007-937 of August 7th, 2007 [6]. According to this decree every subscribers must be identified with its identity card, a passport, driving licensee, school identity card or valid student card, consolidated by a physical presence.

No rigorous control is operated by the competent jurisdictions. The operators are practically alone in this activity. Each one has, from towards him, a system isolated to identify its subscribers. Their system of identification does not have any link with any secure and centralized database. From a portable application, it is enough to indicate a first name, name and a number which respects the nomenclature of the number national identity card which is of 13 digits, to be accepted by the system.

Some subscribers take the luxury to be identified as much they want and to have as many chips as they wish. As the results of the seizures by the Regulatory authority of telecommunications attest some, in August 2015, compared to fraudulent sites: 397 Sim cards and 9 Simbox.

4 SUGGESTED SOLUTION

The proposed solution is composed of:

- platform of identification;
- infrastructure of transmission of the data between the waiter and the users

4.1 Platform of identification

The platform is made up of a database feeding a business application of the subscribers [7]. It will be installed and configured on the waiter accessible by several types of connections through a switch.

4.2 Infrastructure of transmission

This part of architecture relates to the elements of architecture which leave the waiter to go towards the various types of users.

First of all, waiter with the switch, one distinguishes connection RJ45 made safe by a firewall and a router for information bound for the waiter. The switch thus makes it possible to inter-connect the various users with the platform of identification.

On the basis of the switch, the agents of police stations, the police of the borders and/or immigration, are connected by two types of connections:

A dedicated line for the police stations closest to the localization of the waiter [8];

A connection FH for the most distant police stations [9].

The choice of these connections between the switch and the police stations can be explained by the need for availability and speed of service necessary to the police officers to ensure an update in real time of the database with information on the foreign travelers made lately.

In addition, the ministry or the authority, in charge (E) of the identification of the citizens will be requested to feed the database on information concerning the national citizens.

A connection RJ45 will make it possible to the administrator of the platform to be connected to the application by the means of the switch. A router will be set up with a public address to open a way of connection by Internet to the platform for the users “agents of the ORM” in charge of the identification itself with the subscribers. This router will have to be connected to the switch with the other end to indeed ensure an exchange with the waiter.

Agents of ORM will then be able to use all means of Internet access available to connect itself to the application, as indicated on the architecture which follows:

To be identified, the future subscriber must present himself physically to the operator with a part of identification: national identity card, passport, student card or school distribution for the nationals. The foreigners present a passport, a consular map or a student card.

Of the next session of identification, without physical presence, the system, apart from the identification number, requires a password which ensures the safety of the system.

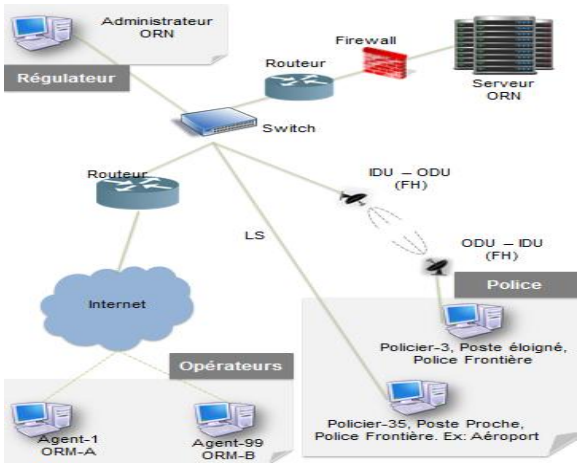

Fig. 1. Global architecture proposed

5 APPLICATION DESIGN

5.1 Modeling of the data

It is a question of modeling a secured and centralized database [10][11] on the level of the Regulatory authority for the management of the identification of various subscribed mobile telephone operators in Senegal. The agents of the operators will be able thus to be connected to the platform to identify the new subscribers whose information including the details of their part of identification (national identity card, passport, residence permit or consular card) will be preregistered by a sales representative, a Policeman of the borders and police station.

5.2 Rules of management

All the citizens and foreigners with the country must be recorded in the database secure and centralized and their information must be updated in the event of expiry of parts of identification (national Identity card, Passport, biometric data or parts authorized). This work is done on the level of the police stations of the borders and police station. The operators and dealers connect themselves on the database centralized to take care of the identification of the subscribers. They can also use a portable application, for the customers who were made identify at least once. A customer cannot have more than 3 chips of the same operator. On the three operators, a customer can only have 9 chips maximum. An operator cannot modify the relative information with customer. Only the regulator (administrator) can conduct such an action. Only an operator can activate a chip with automatic notification with the regulator.

5.3 Diagram of the cases of use

In the diagram of use, the main actors with their principal role are indicated.

- Regulator

The general administrator of the database charged to manage the various users and to parameterize the application. He receives and treats the complaints which are subjected to him by the other users.

The agents of the Body of National Regulation (ORN) will be able to consult if necessary information on the subscribers.

- Organizes

The agents of the operators of mobile network are users who can connect themselves to the platform to identify their new subscribers or another number of the one of their former subscriber.

- Police

The policemen generally coming from the police of the borders or the police of immigration deal with the safeguard of information on the identity from abroad in fan-in on the national territory at the moment even of their arrival. These data which will have to be pre-registered for a phase of identification by an agent of the ORM and must contain the details of identification papers from abroad.

Police Agents at the stations will feed the database according to information of the populations.

The diagram of Figure 2 formless on the interaction between the various actors. Here one identifies the system, the users and the use which it could make of the application. It is noted that all the operations pass by the case of use: “to authenticate itself”. That means that it is necessarily necessary to be connected with its login and its password to

be able to carry out any operation whatever the type of user.

This diagram of Figure 2 presents the existing relationships and associations to their cardinalities between the various entities of the system.

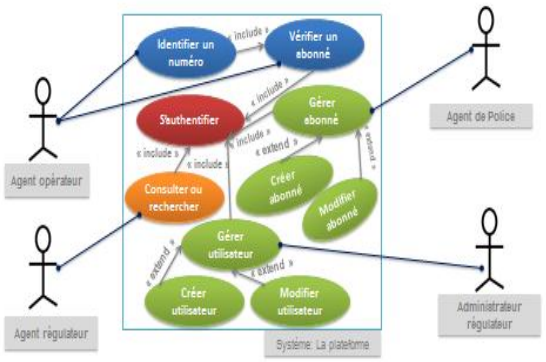

Fig. 2. Diagram of use cases

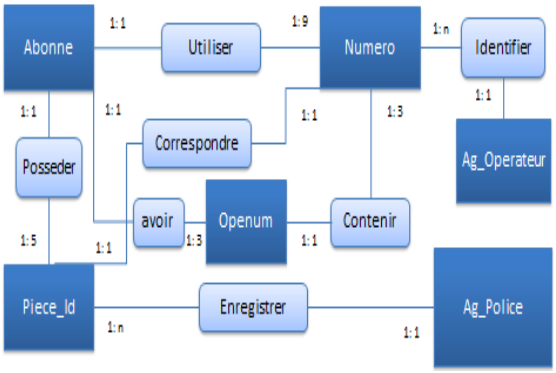

Fig. 3. Diagram of classes

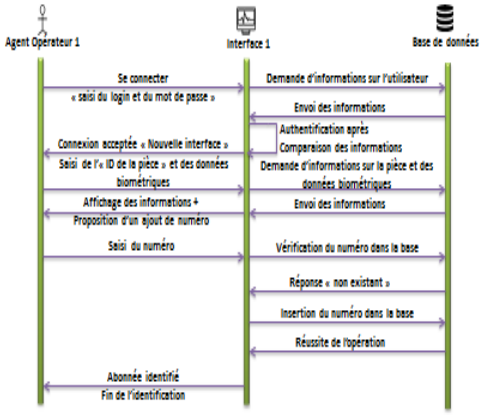

Fig. 4. Diagram of sequence of the case "To identify a subscriber successfully"

Once the identified number, the subscriber will be able to try a call to see whether the chip is activated or not by the operator.

Sequence of the case "to identify a subscriber": case of failure

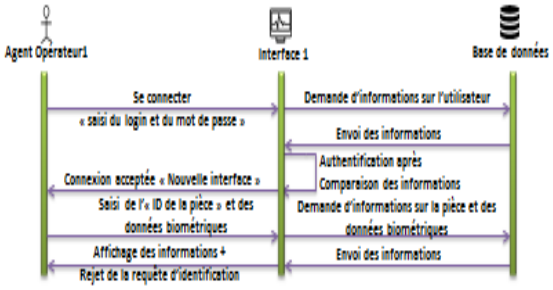

Fig. 5. Sequence diagram of the case "Identifying a subscriber» Stoppers

6 ARCHITECTURE OF SIMULATION

To make sure of better results, it is set up architecture of identification of the subscribers integrating the network 4G which is a recent technology to test activation or not new chips.

The diagram of figure 6 describes the architecture of simulation.

OpenIMScore is the heart of network IMS with the various entities of the CSCF (Call Session control functions) and database HSS (Home Subscriber Server). As for a basic phone network, to join a user requires a single identification of this last in the network. Within IMS, this single identification is realized via three principal elements: IMPI, IMPU, and IMSU [12].

- IMPI (Private To use Identity): used to identify and authenticate an subscriber and no role in the routing of messages SIP plays
- IMPU (Public to use Identity): is provided to the user by the operator of network IMS. The IMPU can be shared with any other terminal user (telephone, softphone, etc.). Thus, a telephone and a softphone can have the same IMPU.
- IMSU (IMS Subscription)

The future subscriber presents himself to the operator. This last seizes the identification number. Application 2 compares the number seized with the number which is on the principal database MySQL. If the two numbers are identical, the system displays with the screen of the operator, first name, names, date and birthplace, addresses, expiration date. If not, an error message is displayed: "number non in conformity, rejection". For a first identification, the subscriber will receive a code pine which will enable him to use a Web application to be identified. He also receives from the operator a chip. The subscriber can validly use the network 4G to test activation or not his new chip.

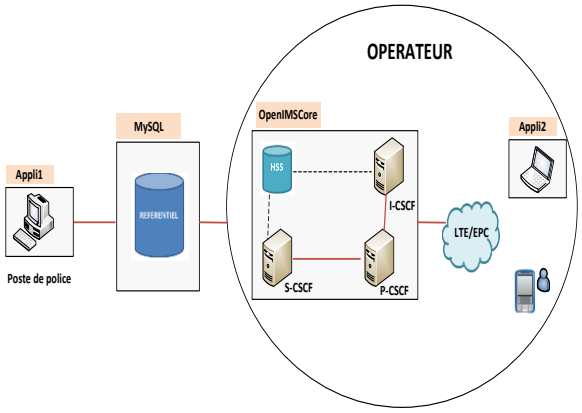

Fig. 6. Architecture of simulation

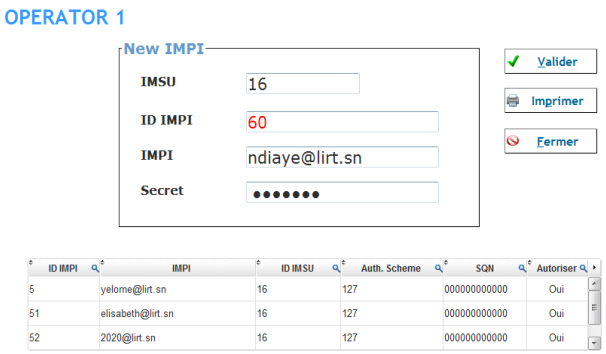

Fig. 9. Adding the IMPI

7 RESULTS

7.1 Some screenshots

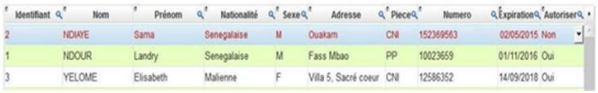

Fig. 7. Viewing the controller database

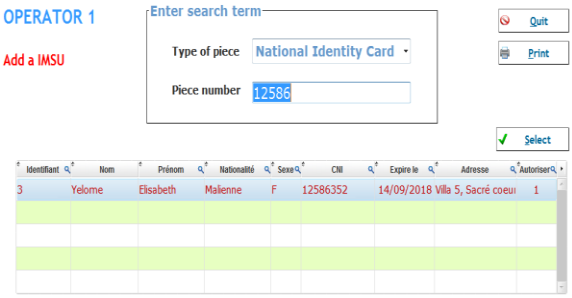

Fig. 8. Adding the IMSU

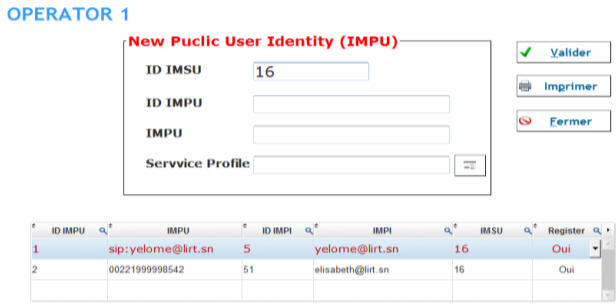

Fig. 10. Adding the IMPU

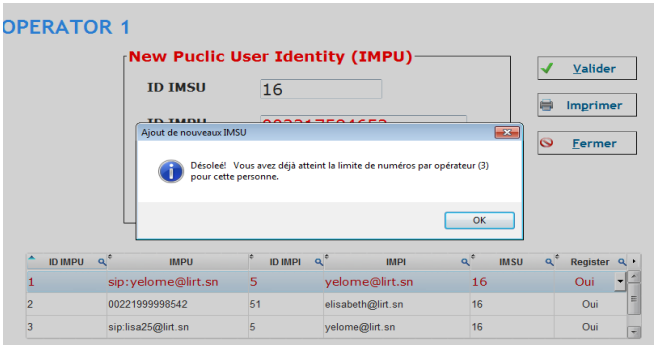

Fig. 11. An attempt to exceed the limit by subscriber number to an operator

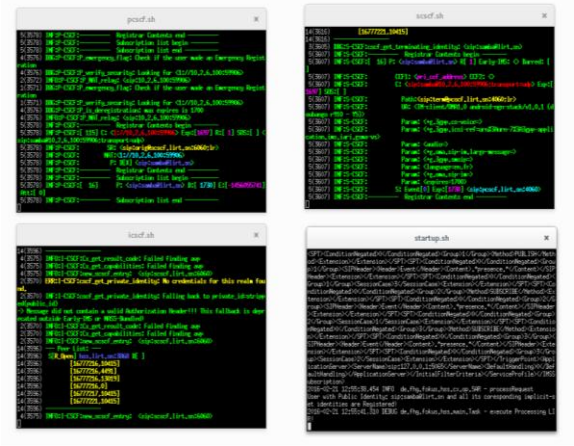

Fig. 12. Reaction of servers when the registration of the subscriber

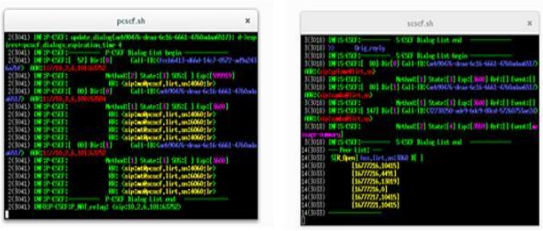

Fig. 13. Reaction servers in a telephone call between registered subscribers

Fig. 14. Terminals showing a phone call between two subscribers

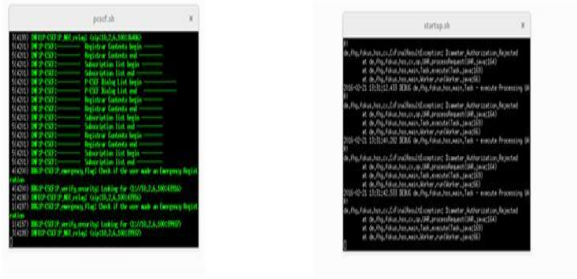

Fig. 15. Recording Attempting unsuccessfully a deactivated subscriber

7.2 Comments and analysis of results

The identification of subscribers constitutes one of the main activities which makes it possible to carry out rigorous and optimal management of the customer who owns each chip. The results above show the relevance of the management of databases maintained by the regulator (Figure 7) and in possession of each operator (Figure 8, 9, 10, 11,12,13,14 and 15).

At the regulator level, the principal database is managed (Figure 7). This database centralizes the sub-bases of data exported based in all the centers of police of the borders and the police stations of proximity. It is put up to date in real time. Information concerns all the people living on the national territory and the people coming from foreign countries. Each person is recorded with her name, first name, birth date, identification papers (standard, number and validity date), etc.

At the operator level, to search a future customer, it is necessary to select the type and to seize the number of identification papers (Chart 8). A request is thus sent to the principal database managed by the regulator. In the event of positive response, the agent proceeds to the registration of the subscriber (Figure 8, 9, 10). Into the contrary case, the registration of the subscriber in the operator is rejected.

The system requires of the operator to respect the number of possible subscription (Figure 11)

Any well registered and active customer can be recorded (Figure 12) and use the services offered in the network (Figure 13.14).

Every subscriber whose validity date of identification papers expired, or prohibited by the regulator or prohibited by the operator will see its account automatically disabled. In this case, it will not be able to be recorded any more, and consequently, it will not be able to use any more the services offered on the network (Figure 15).

8 CONCLUSION AND PERSPECTIVES

The identification of the subscribers to the networks of mobiles answers a national question of security and of maintenance the public order. The system of identification of the subscribers would avoid for example anonymous calls to express or disturb the public order. Taking into consideration terrorism which does not save any part of the world, the identification of the subscribers also takes part of the preventive measures to take. Contrary to the other solutions of identification, the suggested solution is permanent because it covers all the process of attribution and use of the chip in real time. This secure and centralized platform will

thus make it possible to clearly identify the subscribers of each operator and to on the run put an end to the sale chips in the street.

For better making safe the process and fighting effectively against terrorism, the adjoining countries will be invited to also carry out the identification of the subscribers. If not of the nasty people can get SIM cards not recorded in these countries and use them for criminal activities. The isolated efforts of registration would thus not be effective enough. Because of the facility of circulation of the people in the African western area, it is essential to fill this gap by harmonizing the recording of the SIM cards and possibly by sharing this information for the management of the crime in this zone.

9 REFERENCES

[1] http://www.artpsenegal.net/images/documents/Rapport%20T4%202015_VF.pdf, report of the last quarter of the telecommunications regulatory authority and positions (ARTP)

[2] Knake, Robert K. Internet governance in an age of cyber insecurity. No.56. Council on Foreign Relations, 2014.

[3] Broadhurst, Roderic, et al. "An Analysis of the Nature of Groups Engaged in Cyber Crime." An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology 8.1 (2014): 1-20.

[4] Khan, Afaq H., et al. "4G as a next generation wireless network." Future Computer and Communication, 2009. ICFCC 2009. International Conference on. IEEE, 2009.

[5] Hu, Qingmin James, and Douglas Eng. "Architectural model for LTE (long term evolution) EPC (evolved packet core) deployment." U.S. Patent No. 8,565,150. 22 Oct. 2013.

[6] Source ARTP, décret 2007-937, du 07 août 2007, portant identification des acheteurs et utilisateurs des services de téléphonie mobile offerts au public

[7] Kawewirotkull, P. (2015). Invoice verification system for leased line of global information system Ltd.

[8] Cain, S. M., McGinnis, R. S., Davidson, S. P., Vitali, R. V., Perkins, N. C., & McLean, S. G. (2016). Quantifying performance and effects of load carriage during a challenging balancing task using an array of wireless inertial sensors.Gait & Posture, 43, 65-69.

[9] Eum, Doo-Hun. "Design and Implementation of Automatic Script Generator for Mobile Database Applications." Journal of Internet Computing and Services 10.4 (2009): 71-85.

[10] ÖZSU, M. Tamer et VALDURIEZ, Patrick. Principles of distributed database systems. Springer Science & Business Media, 2011.

[11] Gregorovič, L., Polasek, I., & Sobota, B. (2015). Software model creation with multidimensional UML. In Information and Communication Technology (pp. 343-352). Springer International Publishing.

[12] Sun, Lingfen, et al. "Case Study 3—Mobile VoIP Applications and IMS." Guide to Voice and Video over IP. Springer London, 2013. 237-264.