A Multiservice Access Solution based on S-OrBAC Model, Contactless Smartcard and NFC Technologies

Mouad Mammass
LABSI, Faculty of Sciences,
Ibn Zohr University, Agadir, Morocco

Hafid Mammass
Private University of Marrakech
Km-13 route d'Amzmiz
Marrakech, Morocco

Fattehallah Ghadi
LABSI, Faculty of Sciences,
Ibn Zohr University, Agadir, Morocco

ABSTRACT
We present in this paper a multiservice access solution based on S-OrBAC model, contactless smartcard and NFC technologies that allow to benefit from free or prepaid multiservice offered by organizations like universities for example. This solution permits to realize secure micro-transactions, network access and application access.

This paper propose a new variant S-OrBAC model based on the concept of service and the authentication of the cardholder by using the security features of the contactless smartcard and by controlling his rights and attributes stored in the S-OrBAC databases.

Keywords
S-OrBAC, Multiservice access, Contactless Smartcard, NFC, JavaCard, ISO7816, APDU, ISO14443.

1. INTRODUCTION
In large organizations like universities that offer various services, it is necessary to have an efficient infrastructure to manage the access to different resources and services properly. Many works have been done in this field with different approaches. In [1], M. Pasquet and al. presented a technological approach using multiservice IAS smart cards solution as a mechanism with a specific IT infrastructure and access control. The approach of A. Abou El Kalam and al. [2] were based on the access control model Or-BAC in a specific environment like a hospital. F. Layouni and Y.Pollet [3] presented the FI-OrBAC, an extension of Or-BAC, which focus on information and communication systems dedicated to the federated identity infrastructure, in order to treat problems for access control and collaboration.

In previous works [4], we presented a detailed stat of the art on access control models by pointing their advantages and limitations and we concluded that the Or-BAC model was the most evolved one. In fact, this model includes the concept of "organization" and takes the advantages of previous models to build a standard model that makes the organization the central entity with two layers : abstract (role, activity, view) and concrete (subject, action, object).

On another hand, Open JavaCard Cards technology offer the possibility to manage electronic purse and secure electronic transactions. We developed also software to personalize the contact smart card and to use an electronic purse managed by the card in order to pay small transaction amount and to achieve online and offline transactions [5, 6].

In this paper, we develop a solution for multiservice infrastructure based on an S-OrBAC model and contactless cards. S-OrBAC introduce the concept of Service, while contactless card serve as a mechanism for the implementation of the security policy.

In section 2, we present our new variant S-OrBAC model based on the concept of service and that takes advantage of the entity organization. Then, we present generalities about the concept of service and its opportunities.

In section 3, we discuss the contactless smart cards providing the expected features, and a comparative study with the contact smart cards. This comparison is realized on different criteria like technology, cost, security and simplicity.

Finally, we present our solution for multiservice access combining S-OrBAC model and the contactless cards for different application areas.

2. S-OrBAC MODEL
An organization can be defined as a group of individuals with defined role, or as a group of individuals in structured interaction playing specific roles. A high level of standardization and flexibility allows regulating the flow of information (management, database, procedures, etc…) and thus improving the flow velocity and the synergy of the organization.

There are three main types of organizations: private, public and non-profit organizations. There are also other types of organizations such as hybrid organizations that simultaneously operate in the public and private sectors.

An organization cannot exist without a collective goal and without being connected to the external environment that can be the customer, consumer or user. In general, an organization, directly or not, delivers a service.

In this paper, we focus on the integration of the concept of service in the access control model and treat the case of organizations that provide free or paid services to individuals who can be a part or not of these organizations.

2.1 Concept of service
The service consists of providing an intangible, benefit or satisfaction of a need for a service provider (organization or state) to the public, free of charge or expensive from an economic point of view, white in the political sphere, it is reflected in the military or civil service. Finally, in computer science, the service is a feature made available by a software component to provide a specific task.

2.2 Type of service
Services can be classified in four main categories [7] that are differentiated first, by the nature of the service (tangible or intangible action) and secondly, by the service object (person or property).

Table 1. Type of Service

	Person	Property
Tangible actions	Transportation of persons, medical care	Car repair, gardening, …
Intangible actions	Education, entertainment	Insurance, bank account management, …

This study focuses on three visions: economic, political and technological, including different types of services. The concept of service will be adapted in order to meet the needs of the policy architecture and the access control model.

2.3 S-OrBAC Schema

In S-OrBAC model, we consider that an organization is a collection of services that represent structured entities whose purpose is to meet the needs of the end user.

An organization consists naturally of a main business service, representing the principal activity or the purpose of the organization, and many support services that exist to assist the main service and ensure that the final goal succeeds.

To illustrate the pronounced idea, the main service of an IT production company is the production of IT solutions, and the support services in this case, are the accounting service, the human resource service, the commercial service, etc.

Therefore, each service represent several activities that require permissions.

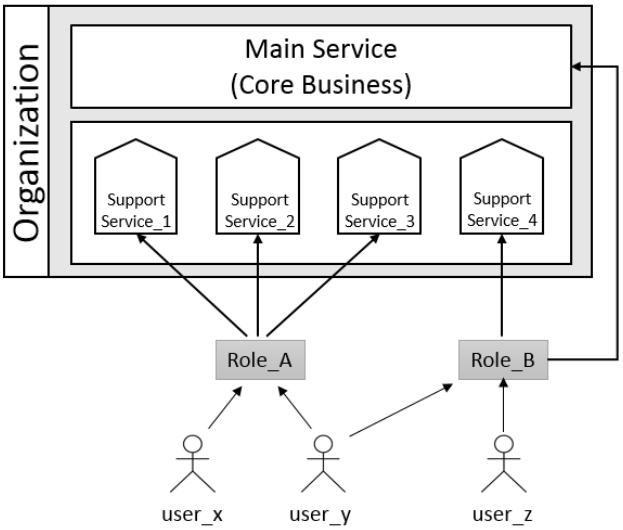

Fig 1: Services representation within an organization and assignment of users

In the example presented above, we assign user_x and user_y to the Role_A, in the same way; we assign user_y and user_z to the Role_B.

The Role_A allows users to perform actions in the support services 1, 2 and 3. The same logic goes for Role_B.

Therefore, a permission is defined mainly by the role and the service.

Assuming that:

- R define Roles
- S define Services
- P define Permissions

For each pair R x S, there is a set of permissions, for example:

$$R\_A \times S\_1 \rightarrow P \{P1, P2 \ldots Pn\}$$

$$R\_B \times S\_main\_service \rightarrow P \{P5, P7 \ldots Pn\}$$

$$R\_B \times S\_4 \rightarrow P \{P1, P8 \ldots, Pn\}$$

Which leads us to have for Role_B paired with service S_main_service, the permissions P5 and P7 for example. In the same way, Role_B paired with service S_4 give us the permissions P1 and P8 for example. Unlike other access control model, we no longer assign permissions to the role, but to the pair role and service.

2.4 S-OrBAC model advantages

S-OrBAC model offer us a new dimension with the new concept of service that gives us many advantages.

First, this concept of service gives us the possibility to bring together the permissions in a specific context so that we have an accurate categorization. The permissions are no longer associated or affected to the roles directly.

This will bring a facility while managing permissions like addition of new permissions to the role, since permissions will no longer be affected to the roles alone but to the pair (roles, services) for more efficiency. From the low-level technical view, the access control model will be more scalable and extensible.

Next, this categorization also specifies a proper lexicon adapted to the policy. For example, if we consider the library as a service, the actions concerned can be: borrow a book, borrow a thesis, access scientific articles, download document, etc. However, in an administrative service, the actions provided can be for example: withdraw a document, signing a document, deposit a document, etc.

Furthermore, the access control and the access to the resources are simplified by using a single mechanism, which allow us to benefit from multi-services. For example in a university, a student will be provided one mechanism that will allow him access to the possible services.

3. SMARTCARDAND NFC TECHNOLOGIES

Our previous works on contact smartcard personalization, ISO7816 protocol and JavaCard proved that these technologies were efficient and very convenient for secure transaction. However, they are very expensive regarding the price of contact smartcard, the cost of developing JavaCard applet ant their installation onto the card and the cost of deployment of these solutions for a big organization.

On the other hand, the contactless smartcards are cheaper and very easier to personalize in a secure mode via simple read, update operation (read and update APDU), and we didn't need to use of JavaCard applet but only maintaining the compatibility with ISO7816 (APDU). Therefore, we can use the same method as contact smartcard despite of the possibility of using ISO14443.

The contactless smartcard technology uses NFC (Near Field Communication) which is an extension of both the RFID (Radio Frequency Identification) technology and ISO-14443 protocol knowledge that the difference between RFID and NFC is the distance between smartcard and the smartcard reader (antenna) supported by RFID (10m) is larger than NFC (10 cm).

3.1 A brief Comparative study between Contact and contactless smartcards.

3.1.1 Contact smartcard

For this type of cards, the energy is supplied by the smartcard reader and the dialog between them is realized by sending respectively request APDU and response APDU.

A contact card has eight contacts and specially a CLK because it does not have an internal clock.

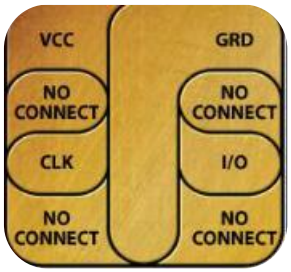

Fig 1: I/O, VCC, CLK contacts

3.1.2 JavaCard technology

JavaCard Language is customized for a smartcard and it is a subset of JavaCard language and because of limited memory resources a JCVM (JavaCard Virtual Machine) is used by this technology in order to respect the JavaCard constraints [8].

In the same time, a JCRE (JavaCard Runtime-Environment) is used by the JavaCard technology for execution of the applet installed on the card [9].

The applets are written in JavaCard language and compiled (off-card) to generate a byte code which is converted (off-card) to cap file which are used to install the applets on the card.

3.1.3 ISO7816 Protocol Description

The dialog between the card and the external world is made by exchanging APDU.

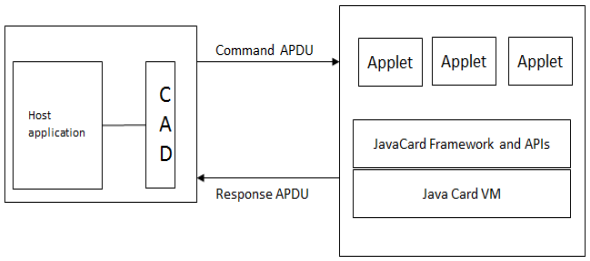

Fig 2: APDU Communication

Commands and the structure of request APDU:

Table 2. APDU Description

CLA	INS	P1	P2	LC	DATA	LE
Class of instruction	Instruction	P1	P2	Length of data	Data	LE

3.1.4 Applet methods

The CAD (Card Acceptance Device) initializes the dialogue with the card, the default applet is selected, and for each received APDU, this applet processes it and sends a response APDU to host application.

The JCRE (JavaCard Runtime Execution) supports the applet execution by analyzing APDU and interpreting them and by executing, the predefined applet methods (select, process, deselect…)

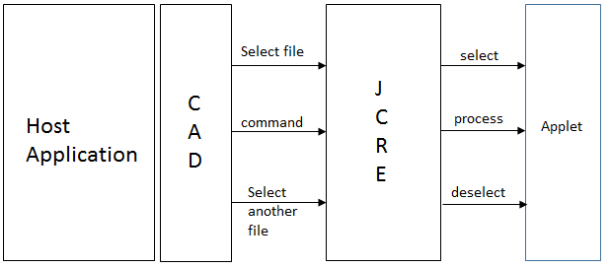

Fig 3: Applet Methods Description

3.1.5 *Contact smartcard disadvantages*

As a conclusion, the contact smartcards are more expensive and are very complex and their personalization software need strong skills and high level of expertise.

In addition, the massive deployment of this technology in a big organization is not possible because of its costs and its complexity and the contactless cards are easier to use and to personalize.

3.2 Contactless smartcard solution

Contactless smartcards are very convenient for application access and control access [10, 11] because the user do not need to provide a pin code or another personal data during a transaction. All the steps of the authentication are made automatically.

A contactless card communicates with the card reader and is powered by it through RF (Radio Frequency) induction technology (at data rates of 106–848 kbit/s). These cards require only proximity to an antenna to communicate. Like contact smart cards, contactless cards do not have an internal power source. Instead, they use an inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics.

APDU transmission via a contactless interface is defined in ISO/IEC 14443-4.

3.2.1 Solution Overview

We have planned to use contactless smartcard to secure the process of Services Access, Network Access and to secure micro-transactions. The cardholder does not need to put physically.

The card into the terminal and to provide a password or confidential data because when the card is on proximity of the antenna, the card will be recognized and the identity of the cardholder will be approved.

3.2.1.1 Authentication keys

Table 3. APDU Request

Command	CLA	INS	P1	P2	P3	DataIn
Authentication	FF	88	0	Block Number	Key Type	Key Number

3.2.1.2 Mifare 1K memory map

The 1K memory of the Mifare card is structured by sectors whose are composed by three data blocks and 1 trailer block.

Table 4. Mifare memory map

Sectors (4 blocks/sector)	3 data blocks(16 bytes/block)	1 trailer block
Sector 0	0x00-0x02	0x03
Sector 1	0x04-0x06	0x07
…		
Sector 14	0x38-0x0A	0x0B
Sector 15	0x3C-0x3E	0x3F

3.2.1.3 Read Binary blocks

In order to read a binary block, we have to send this APDU request

Table 5. Read binary block APDU

Command	CLA	INS	P1	P2	LE
Read Binary blocks	FF	B0	0x00	Block Number	Length expected

3.2.1.4 Update Binary blocks

In order to update binary block data, we have to send this APDU request

Table 6. Update binary block APDU

Command	CLA	INS	P1	P2	LC	DataIn
Update Binary blocks	FF	D6	0x00	Block Number	LC	Data block (16 bytes)

3.2.2 Architecture of the contactless smartcard solution

This solution is based on a client application, which is connected to contactless smartcard reader, this last is waiting for a presence of a contactless smartcard in its proximity. The client application is connected to the S-OrBAC database during the step of authentication and can send requests and receive response to and/from authorization server to realize access attempt to the services or online transaction.

Fig 5: Architecture solution

The main objective is to achieve services access or online transactions by using contactless smartcard for the authentication of the cardholder and the authentication of the card by the issuer authorization server.

A secondary objective is to manage an electronic purse inside the contactless card and then to load a small amount into the card for payment.

Consequently, we have developed a specific interface, which manage the connection to personalization software and to the S-OrBAC database and for achieving some services access attempt to prove our concept.

3.2.2.1 Connection

Two steps make the connection to the personalization software: the first step is to put a contactless smart card in the proximity of the smartcard reader that is already connected to the application and the second step is to connect to S-OrBAC database by introducing users and their associated passwords already parameterized in the database.

3.2.2.2 Human-Machine Interface

This interface offers varied functionalities whose make possible to create an account (Account Management) with initial balance, to create a card (Card Management), and to link this card with the account. Then all access to the resources and services, micro-transaction (Payment by electronic purse) or online transaction are respectively taken in account respectively the S-OrBAC access rights parameterized in the database, the electronic purse balance and the account balance.

The access rights are stored in S-OrBAC database and managed by the access control module, the electronic purse balance is stored inside the card and managed by the card and the account balance is stored in the database and managed by the authorization server.

4. GLOBALARCHITECTUREFORMULTISERVICEACCESS BASEDON S-OrBAC MODEL, CONTACTLESSSMARTCARD AND NFC

The solution aims at providing users with multi-services smart cards, allowing them to access to various resources and services provided by an organization.

The architecture consists of two modules, one for authentication and another one for the access to the different services and resources.

4.1 Authentication and Authorization module

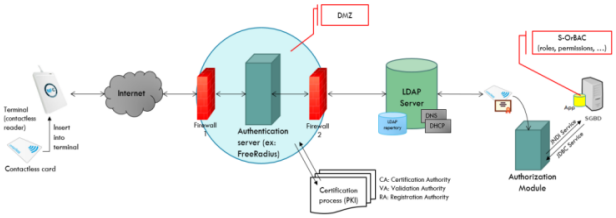

Fig 6: Authentication and Authorization module

This architecture provides strong authentication and authorization through several steps:

1. The user present a personalized contactless smart card at the card reader.
2. The authentication server (e.g., Free Radius) checks the status of the smart card and initiates the certification procedure.

3. After generating the certificate, the identity of the individual is verified with the LDAP.
4. Once the identity is verified, the authorization module engages in a dialogue with the database based on S-OrBAC to verify the roles, permissions, etc. Finally, an authorization is granted for the access to the service.

4.2 Service Access module

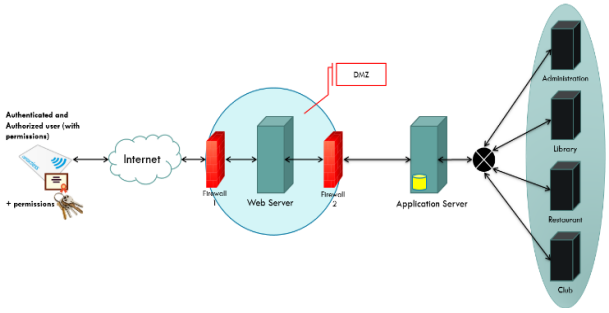

Fig 7: Service access module

This module allows the authenticated and authorized user to access the services permitted by his role, using an application server that redirect him to the desired free or paid service. For the paid service, the user must first have charged his electronic wallet and in this case, there will be a specific treatment related to the type of service, which requires more control and security.

5. CONCLUSION

The paper introduces a global architecture for multi-services access based on new variant S-OrBAC model, Contactless Smartcard and NFC that allows users to access to various resources and services provided by an organization.

The choice of this solution is justified by the fact that S-OrBAC model offers a new dimension to the concept of service with many advantages and by the fact that the personalization of contactless cards needs few skills and medium expertise, their price is cheaper and can be accessible to public institutions such as universities and their students.

In fact, contact smartcards are very secure, combined with modern cryptography are very efficient, and offer a strong mechanism of authentication but they are more expensive than contactless card.

In addition to that, this solution provides an acceptable level of security and uses NFC technology and we believe that connected and mobile objects will make the future and NFC and RFID technologies are respectively strong candidates to assure this challenge.

Future works will present more about the concept of service, and how it affects the other entities within the access control model (action, activity, view, object, etc.) and what will result about it.

As a perspective, we will test the solution on a real case of student services in an institution of the University Ibn Zohr, Agadir, Morocco.

6. ACKNOWLEDGMENT

This work is supported by the National Center for Scientific and Technical Research (CNRST- Morocco) by an excellence scholarship (J 006/009).

7. REFERENCES

[1] Marc Pasquet and Ndiaga Faye; Sylvie Gerbaix "Multi-service Card for Students using JavaCard Global Platform and IAS specifications" Collaboration Technologies and Systems (CTS), 2013 International Conference on 20-24 May 2013

[2] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel et G. Trouessin, Or-BAC: un modèle de contrôle d'accès basé sur les organisations, Cahiers francophones de la recherche en sécurité de l'information, Numéro II, 1er trimestre 2003,pp30-43.

[3] Farah Layouni and Yann Pollet, FI-OrBAC: a model of access control for federated identity platform. International Conference Information Systems, Barcelona, Spain, February 2009.

[4] Mouad Mammass and Fattehallah Ghadi «An Overview on Access Control Models", International Journal of Applied Evolutionary Computation (IJAEC), 6(4), 28-38, 2015

[5] Hafid Mammass and Fattehallah Ghadi 'Implementation of Smartcard Personalization Software 'International Journal of Future Generation Communication and Networking. 12/2012; Vol. 5(No. 4)

[6] Hafid Mammass ; Fattehallah Ghadi and Mohamed Elhajji "Secure Watermarking Method with Smart Card" International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 2– Issue 6, November 2013 www.ijcit.com

[7] Christopher H. Lovelock "Classifying Services to Gain Strategic Marketing Insights" Journal of Marketing Vol. 47 No°3, pp 9-20

[8] The Java Card 2.1.1 Virtual Machine (JCVM) Specification. Sun Microsystems, 2000.

[9] The Java Card 2.1.1 Runtime Environment (JCRE) Specification. Sun Microsystems, 2000.

[10] Mei Jun Voon, Nyuk Hiong Voon, SyMey Yeo, Campus Access Control and Management System, Intelligent and Evolutionary Systems, pp.395-404, 2016

[11] Tayo Arulogun, RFID-Based Students Attendance Management System, International Journal of Scientific & Engineering Research Volume 4, Issue 2, February-2013. ISSN 2229-5518