An IT Application for Student's Access to Services in a University Establishment

Mouad MAMMASS* & Fattehallah GHADI
LabSI Laboratory, Faculty of Sciences
Ibn Zohr University
Agadir, Morocco
mouad.mammass@gmail.com , f.ghadi@uiz.ac.ma

Abstract—We present in this paper an IT Application for student's multiservice access in an university establishment. This application is based on the OrBAC model of access control and the contactless smartcard technology. A case study of this application is presented with some specifications and deployment scenarios.

Keywords-*Access control model; multiservice; university;OrBAC; contactless smartcard*

*****

I. Introduction

The multiservice concept consists of allowing or offering more than one type of service, through a medium, which consists of an entry point to several services.

This support can be an identity card, a USB key, a smartphone with NFC technology, contactless Smartphone, contactless or dual interface (contact and contactless) or hybrid smart card with several technologies.

The concept of multiservice allows the user to benefit from several services via a single identity support. This support permit to authenticate its holder and thus authorize him in relation to its status and the permissions attributed to him by the service provider.

To implement a good multiservice access IT infrastructure, it is necessary to collaborate several technologies such as access control and smart card technology.

Access control refers to the use of mechanisms to enable authenticated entities to perform actions based on their level of authorization and to prevent them from performing unauthorized actions.

On the other hand, smart cards reduce risks because access to applications and networks is only allowed to cardholders who have been issued by the employer service and this after strong authentication between the card and the application or the network and the delivery by the holder of a secret which is verified by the card and which is recorded when the card is personalized.

In previous work, we presented a state of the art and a comparative study on access control models by pointing out their advantages and limitations [1] [2] and at the end of which we concluded that the OrBAC model was the most advanced and comprehensive. In fact, this model includes the organizational concept and takes the advantages of the previous models to build a standard model that makes the organization the central entity with two levels of abstraction: concrete (subject, action and object) and organizational Role, activity, view and context.

In addition, in previous work [3], we introduce an infrastructure based on an OrBAC access control model that integrates the service concept for large organizations that provide services to their employees and customers. In our works, we consider that an organization cannot exist without a collective objective and without being connected to the external environment, which can be the customer, the consumer or the user. Generally, an organization, directly or indirectly, delivers a service.

Based on our previous works [1] [2] [3], we present in this paper an IT application (AppliS-OrBAC) for student’s access multiservice in a university establishment. This application is based on the control model OrBAC and the technology of the contactless smartcard.

In section 2, we present an overview of the concept of service in large infrastructures such as universities that provide services to students and staff.

In section 3 and 4, we present somenotion about access control model and smartcard technologies.

We present in section 5 the infrastructure for multiservice access based on the OrBAC model and the technology of the contactless smartcard.

We propose in section 6 an application prototype (AppliS-OrBAC) for multiservice access in a university establishment that offers others functionalities as personalization, management, etc.

Finally, in section 7, we present specifications and deployment scenarios for our solution.

II. Service Concept

A service consists of "the provision of technical or intellectual capacity" or "the supply of a work directly useful to the user, without transformation of matter" [4].

In computing, for example, the service is a functionality provided by a software component to accomplish a specific task. It is presented in the form of a black box, presenting only its software interface: name of the service, the functions it includes with the input variables required and outputs produced, and any additional informative data on the [5] service.

Services are tangible (Transport of persons, medical care, Auto repair, gardening, etc) or intangible (Education, entertainment, insurance, bank account management, etc) [6].

The services have some intrinsic characteristics [7] as their inseparability from the party offering it, their heterogeneity due to the fact of the human element who is very involved in the delivery, their perishability because its production and consumption occur simultaneously and no transfer of ownership because the service does not become the property of the user.

III. ACCESS CONTROL MODEL

Access control consists in checking whether an entity asking for access to a resource has the necessary rights to do so and is governed by three levels of abstractions:

Access control policy is a high and abstract view of access control. Today, security awareness should also lead any organization to put in place a security policy [8].

The access control model being the intermediate level allowing to link the policy and its implementation and which will allow to support the defined policy [9].

Security implementation mechanisms (Authentication, Authorization and Security of Communication) ensure the availability of information. For example, if an entity wishes to read information contained in an object, the mechanism checks whether that authorization is included in the access control list[10][11].

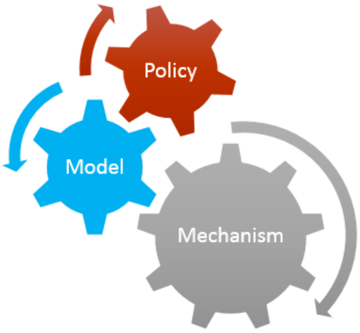

Figure 1. The three levels of access control abstraction.

In previous works [1][2], we presented a detailed state of the art on access control models by pointing their advantages and limitations and we concluded that the OrBAC model was the most evolved one [12][13]. 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).

IV. CONTACTLESS SMARTCARD

Contactless smartcards are very convenient for application access and control access because the user does 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.

The contactless smartcard technology uses NFC (Near Field Communication) which is an extension of both the RFID (Radio Frequency Identification) technology and ISO-14443 or ISO/IEC 15693 protocols 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).

Both ISO / IEC 14443 and ISO / IEC 15693 technologies support access control applications because they have intelligence and are capable of performing read / write operations or calculations. Using these technologies, a person's identity can be authenticated and an appropriate level of access can be deduced. Some cards may also include additional authentication factors such as PINs or biometrics.

V. MULTISERVICE ACCESS INFRASTRUCTURE BASED ON THE ORBAC MODEL AND THE CONTACTLESS SMARTCARD

This Infrastructure based on the access control model OrBAC, the contactless smart card for access to multiservice [3] consists of two modules. The first module for authentication and authorization, and the second to illustrate access to the various services available within an organization such as the university.

A. Authentication and Authorization module

This architecture provides strong authentication and authorization through several steps:

- The user present a personalized contactless smart card at the card reader.
- The authentication server (e.g., Free Radius) checks the status of the smart card and initiates the certification procedure.
- After generating the certificate, the identity of the individual is verified with the LDAP.
- Once the identity is verified, the authorization module engages in a dialogue with the database based on OrBAC to verify the roles, permissions, etc. Finally, an authorization is granted for the access to the service.

B. Mutliservice 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.

VI. APPLIS-ORBAC: PROTOTYPE FOR MULTISERVICE ACCESS IN A UNIVERSITY ESTABLISHMENT

In this section, we present an experimental prototype (AppliS-OrBAC) [14] of access to multiservice for students in an academic institution. This prototype will subsequently be extended to cover other uses and services.

The figure 2 present a sequence diagram of the use case "note presence of the student in examination".

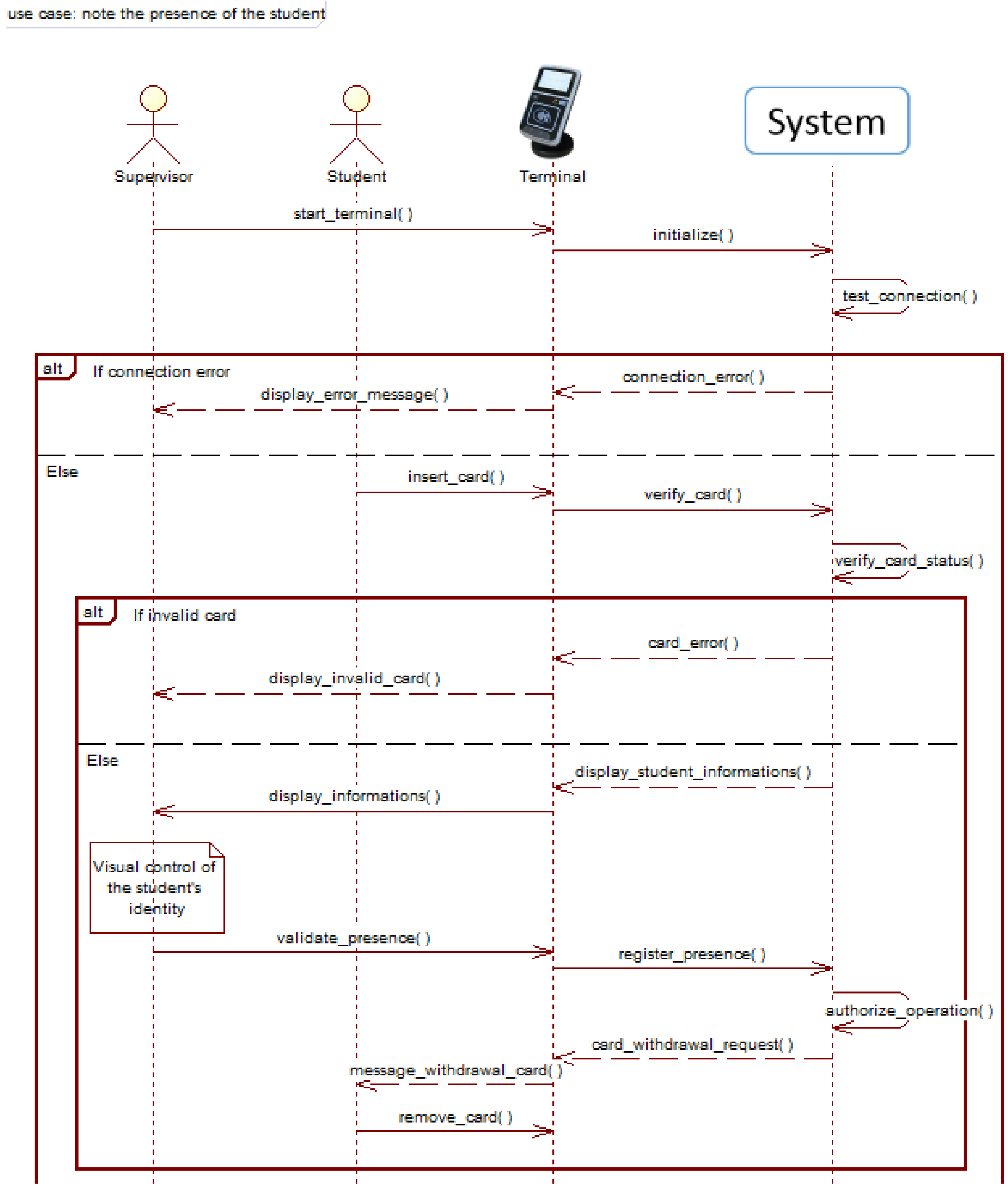

Figure 2. Sequence diagram for the use case "note presence of the student in examination" taking into account different actors in the evaluation process (teachers, supervisors, students ...).

A. Structure of the AppliS-OrBAC prototype

The prototype offers the following features:

- Customizing the smart card and assigning the card to a user,
- Authentication of the smart card and Identification of the wearer,
- Creation of users, services, roles, organizations, permissions, etc,
- Management of users, services, roles, etc,
- Management of different services,
- Viewing user permissions at a service level.

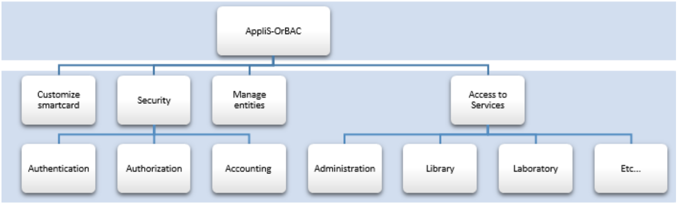

Figure 3. AppliS-OrBAC prototype tree.

B. Flowsheet of the prototype

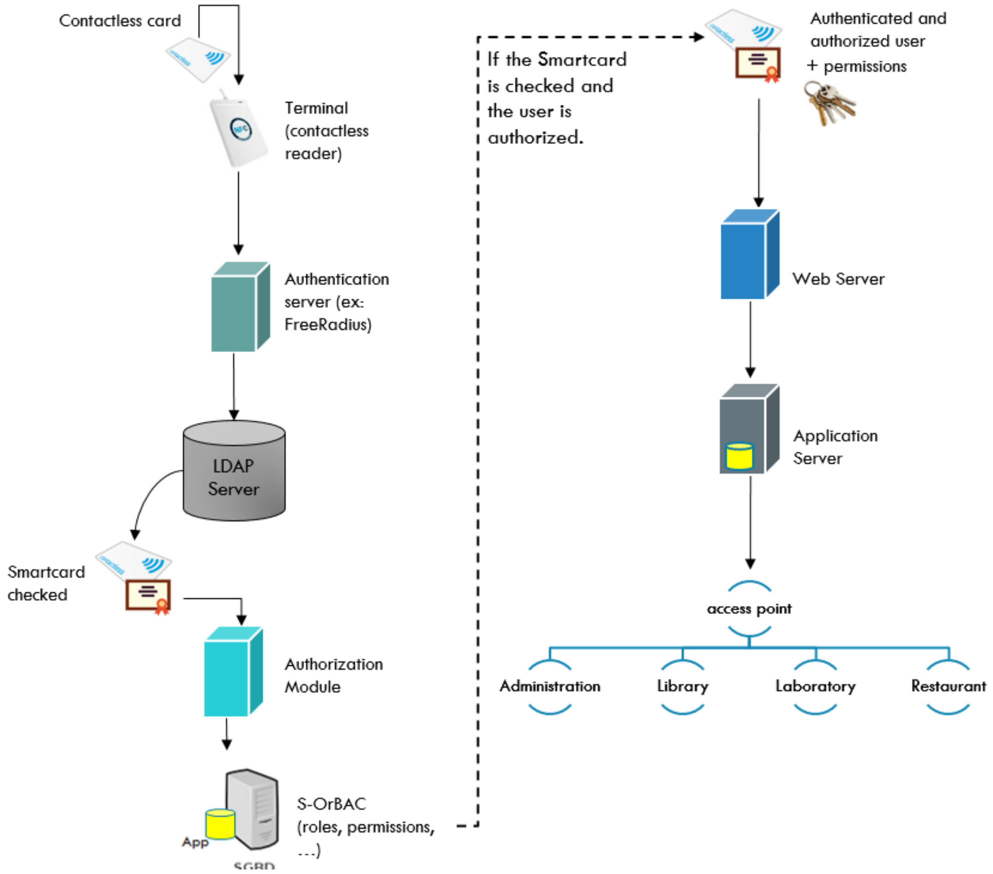
Contactless card
Terminal (contactless reader)
Authentication server (ex: FreeRadius)
LDAP Server
Smartcard checked
Authorization Module
App
SGBD
S-OrBAC (roles, permissions, ...)
If the Smartcard is checked and the user is authorized.
Authenticated and authorized user + permissions
Web Server
Application Server
access point
Administration
Library
Laboratory
Restaurant

Figure 4. Flowsheet of the prototype taking into account the two modules and the application.

VII. Requirements for Deployment in a University Establishment

For the deployment of the AppliS-OrBAC at an establishment of a university, we present a specification drawing the different stages of deployment.

A. *The solution*

The access-to-multiservice solution based on the access infrastructure [3] will be tested initially on a pilot establishment with low numbers

A customizable multiservice card will be distributed to students, teachers and staff as a visual and electronic identification card for the institution, replacing the old media.

It will be a NFC contactless microprocessor card, making it possible to dynamically download applications after the customization phase of the card. The visual of the card includes a photograph of the wearer as well as identification information. The services accessible by this card would be (not limited list):

- control of physical access to certain sensitive premises of the institution (examination rooms, research block, laboratories, workshops, etc.);
- logical access control to the computer network of the establishment;
- access to documentation services;
- access to food services;
- exams enrollment: allow students to start directly with their exam cards. The student will use his card and PIN code at the beginning and end of the exam for authentication. When registering and issuing cards, special attention will be paid to the students on this confidential code and on the uses it may have during the year;
- Terminals for interactive services: in order to give users more autonomy, we want to set up interactive terminals allowing access to (potential) services such as: balancing, updating the card, re-enrolling, Certificate of schooling, transcripts, etc.

This solution has advantages not only for the establishment but also for students and staff:

- University identity card,
- An added value for the University for its Digital Administration.

After the experimentation phase, the project will be spread to the other institutions of university. However, the date of deployment will depend on the study of the financial cost of the solution and the successful completion of the experimental phase.

In order to implement a truly scalable and cost-effective solution for universities, the infrastructure will be connected to the University's Pinnacle database. Card management stations installed at the facility will edit the Java Card for students and staff that will allow physical access control to sensitive premises, logical access control to computers and networks, and access to services.

JavaCard technology provides significant security, and the ability (through Java) to implement applications in a standardized way through applets. The objective is to propose an ambitious, evolutionary and lasting solution.

The main advantage of the JavaCard is that it is independent of the development platform and allows to dynamically unload or update applications on the board in a standardized environment. This allows the applets to be updated. An application can be developed and installed on any platform. Moreover, Java is a high-level object language executable on any operating system. Unlike other cards where programming is done with low-level "physical" languages, the Java Card allows a "logical" programming of the card. Application management operations could then be defined by the Global Platform [HEN 2007] specification, which defines an architecture to securely manage and install programs on multi-application maps (Java Card and other technologies).

B. Management, Enrollment and Peronalization of cards

1) Management

Identity Management: The consultation, search, or modification of users' identities will be based on files, read on media or from databases such as Apogee for students.

Card Management: This will include managing the cards, tracking their inventory and accounting for inventory.

2) Enrollment

This will involve enrolling biometric data, complementary to textual data, such as photography, fingerprinting or signature. This enrollment of data results in the presence of functions related to data capture equipment, specially designed to optimize the tasks of the user and guarantee respect and comfort of the subject. In order to personalize a card with printing of the photo, it is necessary to act on all the links of the scanning chain in order to ensure the quality, and especially as of the acquisition.

3) Personalization

The security mechanism in the Establishment X applet will include encryption of data in the card, access keys and conditions. The data will be stored encrypted or in clear, and their access can be public (by the managers, on login + password) or private (by the holder of the card).

Personalization consists in materializing the identities on media, from the data, in order to allow the identification of people. This materialization consists of printing and encoding media such as badges, cards or labels. From the most basic to the most sophisticated, enabling personalized maps to be obtained with static and dynamic information (texts, images, biometric data);

This makes it possible to control and exchange the data with the local device for graphical and electrical personalization of cards, consisting of a printer and possibly encoding equipment (chip card couplers, magnetic encoder) internal or external to the card 'printer.

VIII. Conclusion and perspectives

This application will allow technology to be no longer a brake to cohabit the different applications. The combination of contactless smart card technology, JavaCard and the OrBAC model and their adaptation to the "multiservice" aspect will enable this challenge to be met. Various uses would be envisaged by the integration of applet services of partners of the university (transport, bank ...) in addition to those specific to the university of course after feasibility studies.

The choice of the contactless card is important, but you have to make sure you have enough memory (10kb per partner) to make the applications cohabit and offer a certain permanence to the card.

Due to the complexity of the deployment of access control infrastructure and card management, a dedicated and qualified service is required in addition to having a provider for the supply aspects of the card.

Finally, this project will enable the implementation of an innovative technology aimed at deploying the multiservice access infrastructure on a larger scale in the coming years with the implementation in the first applet "Establishment". Once the deployment of the access control and card customization functions has been successfully rolled out, the potential of this solution with the possibilities of integrating new applications offers many interesting prospects.

Acknowledgment

This work is realized in a PHD thesis supported by a scholarship of excellence from the Moroccan National Center for Scientific and Technical Research.

References

[1] Mouad Mammass & Fattehallah GHADI ‘Access Control models: State of the art and comparative study’ IEEE 2014 Second World Conference on Complex Systems (WCCS14), Agadir (Morocco) 10-12 Nov. 2014.

[2] Mouad Mammass, Fattehallah Ghadi, "An Overview on Access Control Models", International Journal of Applied Evolutionary Computation, vol. 6, pp. 28-38, 2015, ISSN1942-3594.

[3] Mouad Mammass, Hafid Mammass et Fattehallah Ghadi, A Multiservice Access Solution based on S-OrBAC Model, Contactless Smartcard and NFC Technologies, "International Journal of Computer Applications (IJCA)", Volume 151-number 8, October 2016.

[4] Dictionnaire d'Économie et de Sciences Sociales, Nathan Paris, 1993

[5] Expanding your concept of service. http://www.dummies.com/business/customers/expanding-your-concept-of-service/

[6] Christopher H. Lovelock "Classifying Services to Gain Strategic Marketing Insights" Journal of Marketing Vol. 47 N°3, pp 9-20, 1983

[7] Concept and nature of service https://fr.slideshare.net/NikhilSoares/concept-and-nature-of-service

[8] Trusted computer system evaluation criteria. Rapport technique, 5200.28-STD, DoD Computer Security Center.

[9] AAA (Authentication Authorization Accounting) Authorization Framework, « http://www.ietf.org/rfc/rfc2904.txt?number=2904 », 2000.

[10] F. Chong, brève sur « gestion de l’identité et de l’accès », Site web : http://msdn.microsoft.com/fr-fr/library/aa480030.aspx, 2004.

[11] A. Reed, « The Definitive Guide to Identity Management », electronic book, Real time publishers, 2004.

[12] Anas Abou El Kalam, Rania El Baida, Philippe Balbiani, Salem Benferhat, Frédéric Cuppens, Yves Deswarte, Alexandre Miège, Claire Saurel, Gilles Trouessin, “Organization Based Access Control”, 4th IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'03), Côme, Italie, juin 2003, pp.120-131.

[13] CUPPENS F., MIÈGE A., « Or-BAC (Organization Based Access Control) », DRUIDE, mai2004.

[14] Mouad Mammass, ‘Accès aux services informatiques basé sur un modèle de contrôle d’accès S-OrBAC et les cartes à puces sans contact’ PHD Thesis, Faculty of Sciences, Ibn Zohr University, July 2017, 156p.