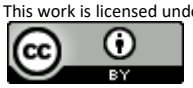
Available online at: https://ijact.in

Date of Submission	25/10/2019
Date of Acceptance	29/11/2019
Date of Publication	30/11/2019
Page numbers	3477-3484 (8 Pages)

Cite This Paper: MoukhlissG., Olaf M., Hilali R., Hicham B., A digital identity security model with smart card and public key infrastructure, 8(11), COMPUSOFT, An International Journal of Advanced Computer Technology. PP. 3477-3484.



ISSN:2320-0790

An International Journal of Advanced Computer Technology

A DIGITAL IDENTITY SECURITY MODEL WITH SMART CARD AND PUBLIC KEY INFRASTRUCTURE

GhizlaneMoukhliss[1], Olaf MALASSE[2], RedaFilali Hilali[3], Hicham Belhadaoui[4]

[1, 3, 4] CED Engineering Sciences, ENSEM, Lab. RITM/ESTC Hassan II
University of Casablanca, Morocco
[2]ENSAM/ParisTech, Metz,France
[1]ghizlane.moukhliss@gmail.com, [2] olaf.malasse@ensam.eu,[3]filalihilalireda@gmail.com,
[4]belhadaoui_hicham@yahoo.fr

Abstract: Nowadays, dematerialization is an integral part of our daily lives, whether in the private sphere, the professional sphere or relations to the administration. The issue of dematerialization includes increased data security against fraud, trust, and the mechanism of cryptography. However, passwords are no longer an effective way to ensure digital identity security for access to digital services within a university. Yet, the use of PKI smart cards is appropriate for strong authentication. In this article, we present the deployment of our security solution, its reinforcement as well as the implementation of some attack scenarios. Our main objective is to ensure access control, authentication and prevent identity theft attacks.

Keywords: digital identity, smart cards, security, access control, Public Key Infrastructure;

I. INTRODUCTION

An information system's security is a critical act[1]. It aims to protect resources from unauthorized use while ensuring access for legitimate users.

In general, information system security has five main objectives[2]: confidentiality, integrity, non-repudiation, authentication and availability.

Confidentiality is about ensuring that only authorized persons have access to protected resources. Integrity is used to determine whether the data has not been altered either accidentally or intentionally. Non-repudiation ensures that a transaction cannot be denied. Authentication is used to prove the identity of an entity. Availability ensures access to information and services. To ensure IT security, several techniques can be used. As part of our work, we are interested in securing digital identity.

In the digital age, identity security requires great importance. It encompasses several aspects such as personal data protection, access control, and protection against malicious attacks.

Authentication is the cornerstone of digital identity. However, traditional authentication by the «login / password" pair is no longer sufficient. Also, identity theft is particularly worrying.

Faced with this situation, several questions arise: how to guarantee the security of digital identity? How to be sure

that this is the right person? What are the security requirements for designing a digital identity model?

In this perspective, we present in this paper our strong authentication solution based on multi-application smart card and PKI certificates. In the second section we present a state of digital identity, after in the third section we present the use of smart cards, in the fourth section we describe the Public Key Infrastructure, in the fifth section we present the electronic notary, in the sixth section we show the role of an LDAP directory in deploying our solution, then we present the implementation in the seventh section, after we propose some attack scenarios in the seventh section, we then end up with a conclusion and some future work.

II. State of Digital Identity

In everyday life, when an individual has to authenticate, he/she is frequently asked to present "his/her papers." Depending on the case, it may be an identity card (for example, to justify signing on a check), a passport (to cross a border), a driver's license (to prove your right to drive a motor vehicle), a professional badge (to justify a right of access to a building), a student card (to access the library), etc.

However, digital identity is well and truly established as one of the most important technological trends on the planet. It can be defined as an identity composed of information stored and transmitted in digital form [3]. Or as a digital representation of an entity in a specific context [4]. It aims to formalize the individualization of access to computer networks, conditioned by the existence of means for verifying the digital identity of users or objects. [5].

Currently, many European countries have adopted an electronic identity document, under the form of a smart card[6]. Some of them are Germany, Austria, Belgium, Estonia, Finland, Italy, the Netherlands, Spain, and Sweden. The purpose of such a choice is twofold:

- Secure the identity card against fraud, by making it more secure complex the manufacture of forgeries;
- Promote the development of dematerialized services, by providing citizens a means of authentication and electronic signature.

Additionally, today, digital identity is an integral part of the fundamental processes of the economic and social order, as several governments around the world, including the United States, Australia and Europe, are moving their services and their online transactions[7]. As a result, the digital identity registered under the national identity system becomes the identity of the individual[8].
The digital identity systems used by governments around the world are based on the one-person principle: a digital identity [9].
Most developed countries now have digital identity systems as part of their government initiatives and many have now adopted the same identity for public and private transactions.[10].
In this online age, digital identity has affected all areas including medicine [11]. Establishing an identity in various digital domains becomes an urgent need [12].
This actually means that digital identity becomes the primary means by which an individual is recognized and can enter into transactions.
Despite all these definitions, digital identity remains a vague concept [13] .

Moreover, for officials and authorities, the main challenge for digital identity management systems is the guarantee of protection and security of private data.
In this context some architectures and protocols have been developed[14]to secure digital identity and build trust [15].
Therefore, cyber security or digital identity security is a necessity. It has issues that go beyond information security alone.

Generally, information security is about protecting the confidentiality, integrity and availability of information. Other properties such as authenticity, accountability, non-repudiation and reliability may also be affected.[16].
However, the traditional method of proving that we are what we say we are in virtual environments - typing a password - is no longer adequate. Indeed, we have too many passwords to memorize; we forget them or write them down.

Unfortunately, we often use easy-to-remember passwords or the same password for multiple accounts; they are therefore easily discovered by other people[17].
In this context is our work, we propose a model to secure digital identity in the academic world.
The proposed solution includes several security measures to protect digital identity from spoofing. We focused on a variety of concepts, including identity and access management[6], cryptography, public key infrastructure and electronic notary.

III. SMARTCARD

To address the issue of digital identity security in our area of expertise, we target the academic world. It is a medium in which different types of actors (administrator, professor and student) have different access rights and benefit from a set of heterogeneous applications or services with varying levels of security.

Authentication is the first step in the process for users to access network resources.
Beyond the traditional means of authentication based on an identifier and a password, our solution is based on the use of a smart card to secure the digital identity against fraud.
Once a user authenticates, the access control defines the resources that this user can access, the actions that can be performed on the resource and whether these actions are audited or not. Access control is implemented by

specifying permissions for resources and objects and assigning rights to users.

In this context, we propose a solution to manage the access control to the various services of a university due to a multi-applications smart card to the users.
Indeed, this solution brings several advantages for the university; first, it no longer needs to issue multiple cards to the same users for different types of access, in addition it eliminates the need to replace cards when rights or privileges change.

Generally, a smart card is a small plastic card containing a built-in chip. The chip is similar to a miniature computer and includes secure data storage including privileges, permissions, private keys, and public key certificates [18].
In addition, smart cards support asymmetric cryptographic algorithms. The chip can store private keys safely. Private keys represent half of the public-private key pairs created to provide the cryptographic functionality that enables PKI applications such as digital signatures and email encryption.

On the other hand, inspired by multi-level security (MLS), we have classified services (applications) into different levels depending on the sensitivity of the service, while ensuring that users only access services for which they are allowed. For this we proposed two access algorithms[19]using smart cards. For sensitive parts of a university requiring a very high level of security (such as the administrative offices and the room where they are deposited and stored exam copies), we defined a contact access. And for services with a medium security level (i.e. access to the restaurant or the boarding school) we use a contactless access.

The principle of smart card authentication with contact is very simple; it looks like the use of a credit card [6]. A user inserts his smart card into a card reader and enters his PIN code. Then the code entered is compared to the PIN code stored on the smart card. If they match, the user is authenticated and can access the desired resource. This type of authentication provides two-factor authentication by checking both what the person has (the smart card) and what they know (the PIN) to make sure they are the right person.

IV. PUBLIC KEY INFRASTRUCTURE

Generally, the network architecture represents the planning of the general organization of computing resources in a coherent network and the secure processing of information. This architecture essentially depends on the resources to be shared and the level of security required.
In this respect, we have proposed a global architecture [20]which is based on a centralized system of identity and access management.

On the one hand, a centralized administration allows us to maintain or increase security while saving time, ensuring more complete distribution of information, managing global access privilege changes from a single point and reducing the complexity of synchronizing multiple systems. On the other hand, it is a security-enhanced, for example in case of departure of a user; all access can be immediately disabled.
The proposed platform is based on smart cards and PKI infrastructures, to provide secure access to the various services of an institution while protecting the digital identity.

First, the access control server receives and correlates the data of the smart card with the data of the database, determines the access privileges of the person and indicates whether the person can be admitted.
To ensure confidentiality and secure data exchange between the smart card and the server we have proposed a cryptographic model [21]based on the PKI architecture.
Generally, the principle of PKI consists in associating two keys (two high primes, thus having no link between them, one cannot be deduced from the other) to a given user: the so-called private one which it is personal and that only he knows and the other known public that can be disseminated to any other person or service. These keys are then used to encrypt any information exchanged using an asymmetric algorithm: the encryption by the issuer is done with one or other of the keys (for example the public key of the receiver) and the decryption with the other key by the receiver (for example the private key of the receiver).
A Key Management Infrastructure (PKI) typically consists of a Certificate Authority, a Registration Authority, and a Certificate Publishing Directory.

The Registration Authority (RA) is an entity that verifies the identity of the holder with a view to delivering a certificate. The verification methods for this step are defined based on the certification policy chosen for the infrastructure. Indeed, this can range from simple email exchange to validate the request or to a verification of the identity of the person (identity card, passport, etc.). If the registration authority validates the registration request, then the certificate request will pass into the hands of the certification authority.

The certification authority (CA) is a moral entity and its main role is to generate a certificate for the user. The certificate will contain personal information about the user but especially his public key and the date of validity. The certification authority will sign this certificate with its private key so that certificate will be certified authentic by itself. This is why we talk about a chain of trust in a PKI because it is to trust this certification authority which will itself be certified by a higher authority and so on. The certification authority will also have the role of updating the list of certificates that it has signed to know the dates of the validity of its certificates. Indeed, to check if a certificate is valid, it will be necessary to ask the CA that it has generated it if the certificate in question is still valid or if it has been revoked.

A Directory: Its role is to store revoked certificates as well as valid certificates in order to have quick access to these certificates. In addition, the directory can store the private keys of the users as part of the key recovery. Knowing that certificates are widely distributed, the directory is a solution to make them available.

V. ELECTRONIC NOTARY

In everyday life, to prove our identity we use written documents such as the national identity card, passport, driving license or other official document. These documents are produced by public authorities and regulated professions acting as trusted third parties.

However, in the digital world, it is the electronic notary, Certification Authority (CA) or even a trusted third party that acts as a notary and allows the verification of a digital identity.

Certification Authorities bind an identity to a PKI-based digital certificate that provides a digital identity guarantee to users. The CA is in fact the legal and moral entity of a PKI.

Indeed, the core of the PKI infrastructure technology is a digital certificate to recognize the network and secure the digital signature.

This digital ID (or digital passport), called a digital certificate, provides a unique digital ID for each individual. It contains the public key of the user, as well as his personal information (name, first name, address, etc.).

Like any formal document, the digital certificate must be signed.

Handwritten signatures have long been used to prove the identity of their author or at least the signer's agreement with the content of the document. For the digital certificate, it is signed by the certification authority and it is this signature that will give it all credibility in the eyes of the users and replace the manual imprint.

The digital certificate is widely published, it does not have to be kept a secret, and it can be consulted via a directory.

In our study, we used Public Key Infrastructure to authenticate users and manage entitlements in the school network.

Generally, the use of a certificate present on a physical cryptographic medium is a strong authentication method. Since we need the support and its secret code (two elements) to authenticate, and that the challenge / response pair changes at each authentication.

Smart cards are an ideal secure storage device. As a result, in our study we use the smart card as a support for the digital certificate.

- Registration phase :

First of all, each new registration in the institution's information system goes through the "registration phase". For this we proposed an algorithm whose principle: The user sends a registration request containing its information and its role to the server. The server makes calculations and generates a random password. Then this information is stored on a new smart card and saved in the authentication server as shown in (Fig. 1).

Then, the smart card system requests a private key from the certificate authority. After verifying the user information from the server, the CA generates a key pair (private and public) for the current user and signs a certificate containing the key pair. Afterwards, the CA sends the certificate and the private key to the smart card and adds the signed certificate to the directory. Finally, the smart card is issued to the user by indicating his initial password.

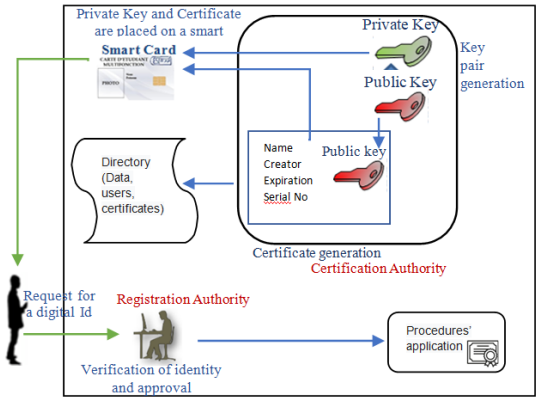


Fig. 1. Certificate request process

- Authentication phase :

When a user wants to authenticate, our authentication system verifies the validity of the card and the code inserted through the PKI architecture. It generates a onetime random number, and then the smart card calculates the encryption with its private key and sends it back to the system. The system calculates the decryption with the user's public key and verifies the correspondence of the two numbers. If this check is true, the server accepts the connection request and grants permission to the user. Otherwise, server rejects the connection request.

In (Fig. 2) we illustrate the authentication process.

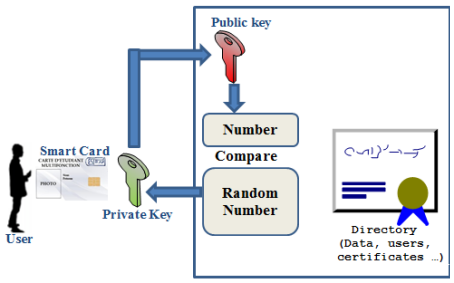


Fig.2: Authentication based on Public Key Infrastructure

The flowchart of the authentication algorithm that we proposed is shown in (Fig. 3).The notation used is defined in Table 1.

TABLE 1: NOTATIONS

Notation	Description
U_A	User 'A'
$Card_A$	User A's smart card
R	A one-time random number created by reader

K	User A's private Key
Y	User A's public Key
E(R)	Random R encrypted with private key K

The authentication steps are as follows:

1. The user U_A inserts his $Card_A$ into a reader.
2. The reader generates R each time. The R number should be as large as possible to avoid redundancies.
3. The $Card_A$ encrypts R with K it contains: E(R).
4. Then, the system checks the certificate information contained in the smart card to verify the user's identity and certificate.
5. Once the verification is done, the system decrypts E with Y: C(E).
6. If the C is identical to R, then the user is authenticated.

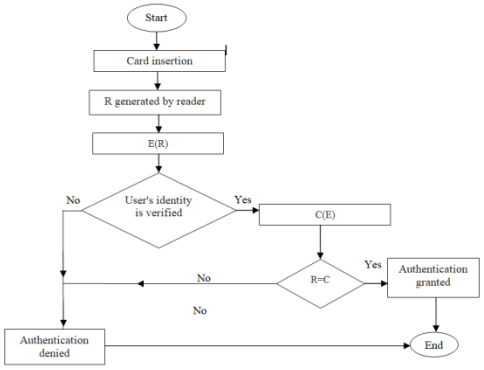


Fig.3. Proposed authentication algorithm

Once authenticated, depending on the roles of the users in the system, a rights matrix [21]has been defined to manage the accesses (grant or reject) to the services.

VI. LDAP DIRECTORY

Now, we will describe the role of the LDAP directory in the management of authorizations for access to the applications of our system.
The management of access rights describes on the one hand, the access rights of users to the applications (or services) of the institution and on the other hand to control access to them in compliance with these rules.

The description of access rights depends on several parameters such as the role of the user, the type of network he uses, or the workgroup he belongs to.
Application access control is performed when the user requests access to a given service after successful authentication. In this sense, an LDAP directory is a repository of authorizations to interpret security rules and control access to applications.

An application is none other than an information system resource. It can be described in the LDAP directory just like any other resource (a printer or a computer).
Because the LDAP directory follows the X.500 model[22], the schema of the proposed directory represents a hierarchical organization of the data (root branches, leaves) reflecting the organizational model of the institution. This facilitates access control to the set of applications based on the profiles of each user.

From this fact we first created dynamic user groups, and then we grouped the rights in the form of "profile". Finally, we assigned rights to a group rather than an individual, as shown in (Fig. 4).
Based on the hierarchical structure of an institution, we defined three profiles:
- A student profile;
- A teacher profile;
- An administrative profile.

In addition, the profile will then be conjugated, in an application way, with the entity of belonging (group) of the user, so as to bring an additional filtering in the management of access rights to the applications. For example a student profile is strictly forbidden to access the room where are stored copies of the exams, or to access the offices of the administrative, on the other hand he has the right to access the laboratory, the restaurant or a room review. Still a teacher profile cannot access the director's office for example.
Then, we associate each profile with our used means of identification: a smart card.

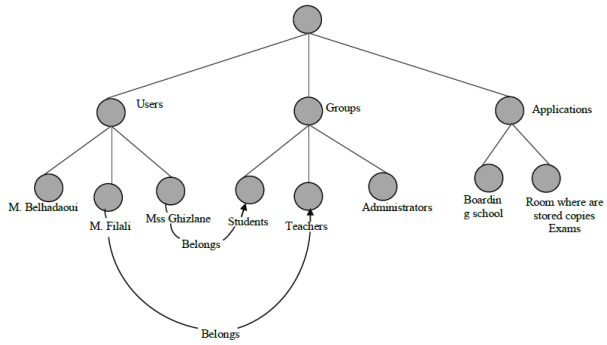


Fig.4. Authorizations in LDAP directory

Additionally to the authorization management, the LDAP directory allowed us to store digital certificates (Fig. 5).
Indeed, in public key architecture, it is essential that certificates can be shared between the different actors[23]; these may be natural persons, certification authorities or computer applications. It is therefore necessary to have a tool based on an open standard to save certificates and read them from different search criteria, such as the name of a person and the name of a service, but also of access it from anywhere and from any type of tool and platform. In this respect we use LDAP directories, as long as they are well suited to this need.
Once the certificate is generated by the Certificate Authority, it is transmitted to the bearer and also published in the LDAP directory.
Because the PKI allows you to revoke certificates, the CA adds them all to the revoked certificates (CRL) list and also

stores them in the directory so that you can refuse the validity of a certificate if necessary.
In an LDAP directory, the cornerstone of security solutions, electronic certificates make it possible to effectively find the identifiers of a given person.

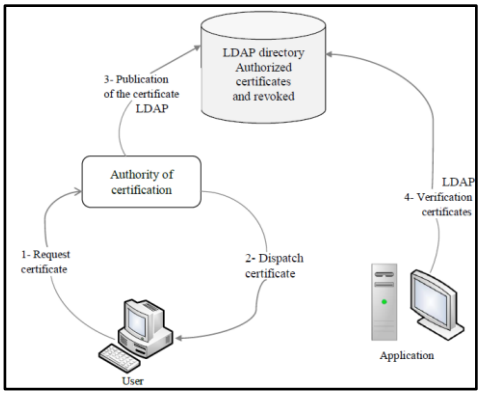


Fig.5: Storing certificates in the LDAP directory

VII. IMPLEMENTATION

To implement our solution, we have set up an OpenLDAP directory server in a virtual machine that hosts a Linux OS. Then, we defined its tree structure.
The structure chosen for this tree (Fig. 4) is based directly on the division of an example of an establishment into components for profiles (Administrators, professors and students), users and services by creating a branch for each. This structure (Fig. 6) simplifies access control rules because it allows you to associate a given user with a profile and then with a specific service.

```
# extended LDIF
#
# LDAPv3
# base <dc=Est,dc=com> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# Est.com
dn: dc=Est,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: Est
dc: Est

# admin, Est.com
dn: cn=admin,dc=Est,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# groups, Est.com
dn: ou=groups,dc=Est,dc=com
objectClass: organizationalUnit
objectClass: top
ou: groups

# users, Est.com
dn: ou=users,dc=Est,dc=com
objectClass: organizationalUnit
objectClass: top
ou: users
```

Fig.6: Structure tree

We used phpLDAPadmin to manage the LDAP server as shown in Fig.7.

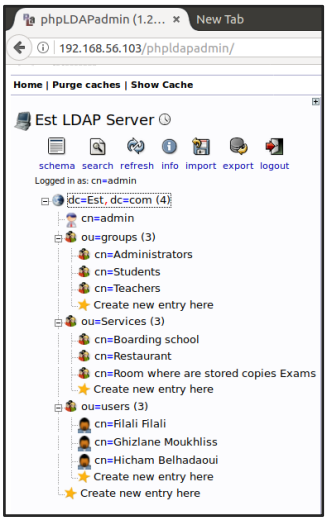


Fig.7: Phpldapadmin interface

Then we activated Openssl in OpenLdap.
First of all we generated a self-signed certificate (Fig. 8) with the private key for the server:

```
root@server:/etc/ldap/ssl# openssl req -newkey rsa:2048 -x509 -node
s -out /etc/ldap/ssl/certs/slapd.pub -keyout /etc/ldap/ssl/private/
slapd.key -days 3650
Generating a 2048 bit RSA private key
.....................+++
.............+++
writing new private key to '/etc/ldap/ssl/private/slapd.key'
-----
You are about to be asked to enter information that will be incorpo
rated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MA
State or Province Name (full name) [Some-State]:Casa
Locality Name (eg, city) []:Casa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EST
Organizational Unit Name (eg, section) []:GI
Common Name (e.g. server FQDN or YOUR name) []:Est.com
Email Address []:ghizlane.moukhliss@gmail.com
root@server:/etc/ldap/ssl#
```

Fig.8.Self-signed certificate

The private key generated is shown in (Fig. 9).

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDAThNeDADH7BAD
SGvbfbkFVwdO3SxhqHYkHeMGyawSEbx5VQCbnQ0SNDujfIFnz7TI3aNAC8Gmt/YB
GJXuwtELH88Mt0S+To28A4ChbEiqVWVAfmro7tLNoHClXP9NtJRlLQp6+WZr8gl2
p8eWedReVxrqmXcOiabXczEntdV3zfSdCo52Mi9Hm1otleMHgoVWTZupp/rhVBJ7
vkIONLcci2xERgh7MyAtH4oxy8eSwzaSAnYkpf0OrKqwnm6jiTOr3Xu3CCdDOYAp
fp7nGEWWOzY/eHUDjBlzn4mhCsVIrcKOJOXy9xzw3Kf+W2XLLzyVxNux1F4/LW+R
NdBsBkcjAgMBAAECggEBALr2LVYuDURReW/3pQUMQimy5uQBm/iGM/YBKIuc3rHi
lH7R6XlhQygDqEfV8GnhQj5XXTQTOf7As2d1Y69xsJNEJaSTOT5cWOgF77UA9dTE
mWAOiBpWtpQ7+8iJlZ0Sh4OmOp48gxtHgXPewujFIXdm8EBNW7bClXa6A3w8CIIk
BtHEYnqzUpQneWX1bvnAK6Pvr5uI4R0dMnTlVbM9s5bxO+DXoikmZzKMS3c5Htit
gucNjkdE5C+lCQdvN779qMin139wcLt+hcw0U50yq+CENMLYJquF2DF/D36QzCie
eY2eMiEB/r+X1HqwwiHW1uC1jRPD5KkwwIcyXbXsz4ECgYEA3u4JQmjSTEwJXQFn
vcdi9YDjr2lCoX0r0ZACGIQdoXrn76B940jlyzbaMOdpJzOAS1xAlE6Mwt7mt3ES
5zM45R7Nb5KfKCq4UN22cLNBVK9dk9UE9wvcXdzbOtxe6F5zpeDyGb3KURgR7pS6
fkotcjSlVmPISAtldHKGhIHFSFMCgYEA3NUIcqSliNta6ARYGp1TBED7VoSqNlDM
T7Ky4PFmJN1Kwwo0zrat4w+NmOs5gflaDA634WYqR/lBIlXVv+unyK8I8XuY54T0
9RMjWpG8MawoKwacygzqIxdCj1oynChtsTUQ/BJAY2B828NRTL4niggaNcM8QDE4
XFn+CtdT6/ECgYASTPAtp3U8FjHelLLzfV6+UKpgR//USfZC6dOCN7ZG/1Py8/Xh
pqZWnFYlFZooQa4Sgaw7gIdFqA7AmGO43xeYl4K92gd+wKMI4GqNrel7DjpcXGxf
63VXrz3AAz83TCmqQGEfg9kL9zHhqAv3Oheo/HFmOiLC50yY1p38WrrbSQKBgC5C
znc9uJO36A5MwqwoovhOKHLSbdndCT/03nYy+8PjO8MqAy/+ouS7IF2VgUGSG+QE
vU6RmW/kblmkA5gl5Mssp8H2s2xktPAWJ0TU3MjHGM8SnovRMsdRGxduvMVrzrbd
uAYmSKjI0L805nYeK6hF1D/I+3kzFmx6Sba5rxHxAoGAQwCe8VzZjkp//9FgPKJq
lU+k3SV6Act66KRHvf1N6Qd3cJ6wzhXOMkYjIiUeNMxmIE+LkLA5m2+qenbQ3rgR
9A8lQiFfG5JwVKf/J8JxnBjr8tXyXcp1b6eR/RASPe5EbFg9o5DkzGhrb1aNNtIT
EwSEp/rGvO4cON5m5axqr6A=
-----END PRIVATE KEY-----
slapd.key (END)
```

Fig.9. Private Key generated

The generated certificate is shown in (Fig.10).

-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIJAIWiffTKoZJFMA0GCSqGSIb3DQEBCwUAMIGFMQswCQYD
VQQGEwJNQTENMAsGA1UECAwEQ2FzYTENMAsGA1UEBwwEQ2FzYTEMMAoGA1UECgwD
RVNUMQswCQYDVQQLDAJHSTEQMA4GA1UEAwwHRXN0LmNvbTErMCkGCSqGSIb3DQEJ
ARYcZ2hpemxhbmUubW91a2hsaXNzQGdtYWlsLmNvbTAeFw0xOTEwMjAyMzA0NTRa
Fw0yOTEwMTcyMzA0NTRaMIGFMQswCQYDVQQGEwJNQTENMAsGA1UECAwEQ2FzYTEN
MAsGA1UEBwwEQ2FzYTEMMAoGA1UECgwDRVNUMQswCQYDVQQLDAJHSTEQMA4GA1UE
AwwHRXN0LmNvbTErMCkGCSqGSIb3DQEJARYcZ2hpemxhbmUubW91a2hsaXNzQGdt
YWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMBOE14MAMfs
EANIa9t9uQVXB07dLGGodiQd4wbJrBIRvHlVAJudDRI0O6N8gWfPtMjdo0ALwaa3
9gEYle7C0Qsfzwy3RL5OjbwDgKFsSKpVZUB+auju0s2gcKVc/020lGUtCnr5Zmvy
CXanx5Z51F5XGuqZdw6JptdzMSe11XfN9J0KjnYyL0ebWi2V4weChVZNm6mn+uFU
Enu+Qg40txyLbERGCHszIC0fijHLx5LDNpICdiSl/Q6sqrCebqOJM6vde7cIJ0M5
gCl+nucYRZY7Nj94dQOMGXOfiaEKxUitwo4k5fL3HPDcp/5bZcsvPJXE27HUXj8t
b5E10GwGRyMCAwEAAaNQME4wHQYDVR0OBBYEFBBtN/IIxA6uqn7t5TUJiAJThXMZ
MB8GA1UdIwQYMBaAFBBtN/IIxA6uqn7t5TUJiAJThXMZMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQELBQADggEBAFcwkYOI9oSACmeI/XPg3+wm0RPGZDrMNjM5mRo3
h1scTx77QDCbIGR9LimdoMVlOSXpjMxddbGJmaoOoi3wc2L7jooEFMc/zZKrsrV9
pJXHDVI1nuXYYM7t5Q+sI9IU4bPPH3vcoAQUxFoYpMZz8OyJqy8egCuumquqwU3f
rwXKloaBIzTi+SPmIY7oYfFRb/f4LIh1pVWOZJ0lI0vY9s35jK/jddv0XFAZT03d
6zK6s34cFqPw6ax2P+rICTXyLnusLIndkzaCU3kjpn+lcMy2kLGswmV/05HxYa3j
RGePOjMBzDUjMwYb4IWZflgHt5+J3zoLsGasZ6kznJRTbkM=
-----END CERTIFICATE-----

Fig.10.Generated certificate

Then for each user we generate a key pair and a certificate. The certificate and the private key are stored in the smart card.

VIII. Attack Scenarios

The authentication system we offer reduces fraud. But it does create new problems. Indeed, the loss or theft of the card.

To subject our approach to security evidence, we have developed three attack scenarios.

The smart card represents the base unit in an attack scenario.

To design and implement the necessary and appropriate attack scenarios to detect and respond to the types of threats we have done three scenarios:

A. Limit the number of attempts

To protect the use of the smart card, it is therefore essential to limit the number of attempts to insert the PIN code. For this, the system that we proposed accepts only three unsuccessful attempts of authentication.

On each erroneous test, the system displays the number of attempts remaining.

If the user exhausts the three PIN identification attempts, the system refuses any further authentication attempts and the card will be blocked until an administrative action is taken.

In figure 11, we schematize the authentication algorithm with smart card and show the counter of the attempts.

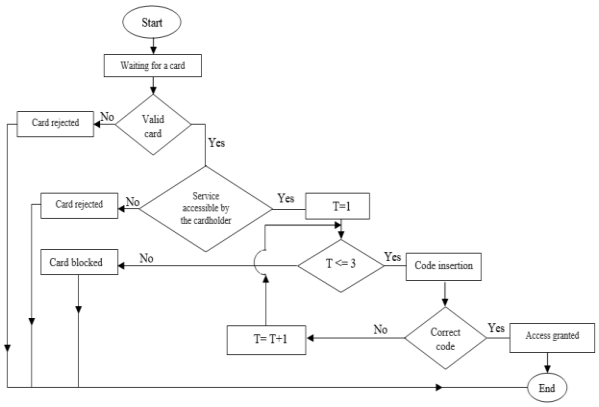


Fig.11. Proposed authentication algorithm

B. In the case of Stealing

In this scenario, the user's card is stolen or lost. The user must immediately contact the schooling service. After making a declaration of loss, the card is blocked.

This statement will have many implications for the map. Examples include the suspension of access rights to the card in controlled buildings and halls of the institution, the suspension of access rights to examination rooms and the revocation of digital certificates related to the owner of this card.

Once a card is declared lost or stolen, a new card will be automatically ordered, and the user can withdraw his card from the schooling service. All rights related to the old card will automatically be transferred to the new one. In this respect, our proposed security system is centralized.

C. In case of use by another person

We seek to reduce the risk of fraud on all levels. For example, in case a user lends his card to his friend. In this case, strong authentication by three factors strengthens our security system. This is to complete the authentication by smart card and PIN, by entering an OTP.

By sending a Short Message Service (SMS) to the user's phone, including a server-generated One Time Password (OTP), we benefit from enhanced security for all connections and access to our system.

With the OTP SMS, we send a temporary password that is only valid for a transaction. It addresses some of the shortcomings associated with traditional static passwords, such as vulnerability to replay attacks. It cannot be memorized by humans.

Since this requires use of a phone not necessarily a Smartphone.It is a solution within the reach of all users, it is not expensive.

(Fig. 12) shows the scenario of such authentication, by smart card and OTP via SMS:

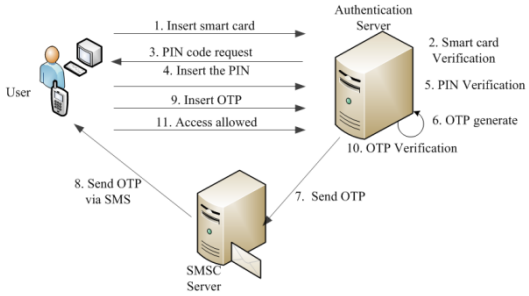


Fig.12 .Authentication SMS / OTP

First, the server checks the smart card inserted by the user. The latter enters the PIN code. After verification of the PIN code, the server generates an OTP, then sends it to the SMS-C, which retransmits it via SMS to the user's phone wishing to authenticate. The user opens the SMS and reads the OTP, and enters it into the authentication interface. The OTP is sent back to the server, proving that the user has his phone.

IX. CONCLUSION

In this paper we presented a new approach for securing digital identities and access control to university services.

Our proposed approach is based on multi-application smart card technologies and Public Key Infrastructures. Since PKI represents an environment in which a certificate authority guarantees the digital identity of users.

To ensure security, we used strong authentication, efficient cryptographic protocols and a digital certificate. Indeed, a digital certificate is the primary means by which an individual is recognized and can perform transactions under the system. This certificate is stored in the smart card of the user and an LDAP directory.

Access management is based on user profiles, in this sense we have defined three profiles (students, professors, administrators) according to the actors of an institution, for each profile a set of rights is defined.

As perspective, we will focus on the continuous online authentication system to verify the user's identity and detect incorrect behaviours continuously throughout the online evaluation process.

X. REFERENCES

[1] Pernet, C., 2015, Sécurité et Espionnage Informatique : Connaissance de La Menace APT (Advanced Persistent Threat) et Du Cyberespionnage Ed. 1, Eyrolles, Paris.

[2] Audit, conseil, installation et sécurisation des systèmes d'information, Éd., Sécurité informatique: ethical hacking apprendre l'attaque pour mieux se défendre, 3e édition. St Herblain: Éd. ENI, 2012.

[3] Sullivan, C., and Stalla-Bourdillon, S., 2015, "Digital Identity and French Personality Rights – A Way Forward in Recognizing and Protecting an Individual's Rights in His/Her Digital Identity," Computer Law & Security Review, 31(2), pp. 268–279.

[4] El Maliki, T., and Seigneur, J.-M., 2013, "Chapter 71 -Online Identity and User Management Services," Computer and Information Security Handbook (Third Edition), J.R. Vacca, ed., Morgan Kaufmann, Boston, pp. 985–1009

[5] Laurent, M., Denouël, J., Levallois-Barth, C., and Waelbroeck, P., 2015, "Digital Identity," Digital Identity Management, London, ISTE Press, Elsevier, pp. 1–45. https://doi.org/10.1016/C2015-0-00282-9

[6] Mouton, D. et.al., 2012, Sécurité de La Dématérialisation : De La Signature Électronique Au Coffre-Fort Numérique, Une Démarche de Mise En Oeuvre Ed. 1, Eyerolles, Paris.

[7] Sullivan, C., 2014, "Protecting Digital Identity in the Cloud: Regulating Cross Border Data Disclosure," Computer Law & Security Review, 30(2), pp. 137–152.

[8] Sullivan, C., 2009, "Digital Identity – The Legal Person?," Computer Law & Security Review, 25(3), pp. 227–236.

[9] Sullivan, C., 2018, "Digital Identity – From Emergent Legal Concept to New Reality," Computer Law & Security Review, 34(4), pp. 723–731.

[10] Gill, B. C., Zampini, A. M., and Mehta, N. B., 2015, "Digital Identity: Develop One Before You're Given One," Urology, 85(6), pp. 1219–1223.

[11] Samia, B., and Maryline, L., 2015, "Digital Identity Management," Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands.

[12] J. L. Camp, "Digital identity," in *IEEE Technology and Society Magazine*, vol. 23, no. 3, pp. 34-41, Fall 2004. doi: 10.1109/MTAS.2004.1337889.

[13] Mui, L., Mohtashemi, M., and Halberstadt, A., 2002, "A Computational Model of Trust and Reputation," Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 2431–2439.

[14] Cameron, K. (2005), The Laws of Identity, published as weblog.

[15] "ISO - ISO/IEC 27000:2016 - Technologies de l'information — Techniques de Sécurité — Systèmes de Gestion de Sécurité de l'information — Vue d'ensemble et Vocabulaire" [Online]. Available: https://www.iso.org/fr/standard/66435.html. [Accessed: 23-Sep-2019].

[16] P. Simmonds, "The digital identity issue", *Network Security*, vol. 2015, no. 8, pp. 8-13, August 2015.

[17] Karray, A., 2008, "Conception, mise en oeuvre et validation d'un environnement logiciel pour le calcul sécurisé sur une grille de cartes à puce de type Java," p. 167..

[18] Ghizlane, M., Reda, F. H., and Hicham, B., 2019, "A Smart Card Digital Identity Check Model for University Services Access," Proceedings of the 2nd International Conference on Networking, Information Systems & Security, ACM, New York, NY, USA, pp. 67:1–67:4.

[19] Ghizlane, M., Reda, F. H., and Hicham, B., 2018, "A Security Policy for Access Control to Academic Services Based on Public Key Infrastructures and Smart Cards," 2018 6th International Conference on Multimedia Computing and Systems (ICMCS), pp. 1–6.

[20] Moukhliss, G., Hilali, R. F., Belhadaoui, H., and Rifi, M., 2019, "A New Smart Cards Based Model for Securing Services," 17(1), p. 15.

[21] Rizcallah, M., 2004, Annuaires LDAP Ed. 2, Eyrolles, Paris.

[22] Cloux, P.-Y., and Corvalan, R., 2004, Les annuaires LDAP: Méta-annuaire et e-provisioning, Dunod, Paris.