Identification System using Mobile Device Enabled NFC

Karima Maazouz
Student,
Analysis, Modeling and Simulation Laboratory,
University Hassan II, Morocco.

Habib Benlahmer
Professor,
Laboratory of Information Technology and Modeling,
University Hassan II, Morocco.

Naceur Achtaich
Professor
Analysis, Modeling and Simulation Laboratory,
University Hassan II, Morocco.

ABSTRACT
Smartphone are becoming more deployed, and such as a way for identification and authentication. The personal identification on mobile devices has attracted a lot of attention in the few years. In this paper we propose an identification system based on Smartphone enabled NFC. The idea is to combing the characteristics of the eID card with the NFC technologies using the mobile phone. The proposed solution must be carried out in a secure way since it can be involved in different services such as m-commerce and e-Gov in local modes.

Keywords
Mobile-ID; NFC ; e-ID; E-Government; security.

1. INTRODUCTION
Mobile phone have evolved from being a device of voice conversation to powerful mobile computer which offers users data connectivity but also a wide variety of technologies such as cameras, GPS and near field communication. The Smartphone as a platform had huge potential, it can provide pervasive access to the internet through 3G and 4G networks, and more importantly it is a device people carry around almost everywhere they go. Furthermore, the Smartphone is a device which is still, evolving. Currently new Smartphone are entering the market with technology such as NFC (Near Field Communication). NFC will allow the Smartphone to wirelessly interact with physical object will enable the phone to simplify the daily life for its users. NFC can seamlessly receive and transfer information which would otherwise be tedious work for the user to input. Currently the majority of the education institutions in the world reply on student identification cards for identification purposes[2]. This includes authorization of access to school facilities and resources. The M-ID system addresses the problem for authenticating system using the Smartphone. The citizen hold his ID card on his Smartphone in order to be identified in different services from the commerce services to government services. NFCs capabilities enables the Smartphone to become a platform for identification, which in turn can be used to access public services such as school services, transportation services and eventually even health care services. The Smartphone has the potential to become a multi-identity platform[4]. In this article we envision the Smartphone in a mobile identification card (M-ID) scenario the immediate benefits of the M-ID system will be a reduction in the expenses paid be services authorities for creating and distributing plastic citizen ID cards containing RFID chips and magnetic stripes, it remove the need for carrying a card only usable for citizen ID.

Furthermore, for the services providers perspectives it will provide a trustworthy mechanism to authenticate citizens eligible. One of the most visible challenges for mobile eGovernment applications has been the lack of NFC phones capable of supporting secure e-Gov applications[3]. A key requirement for government adoption is to have capable phones broadly deployed. The rest of the paper is organized in the following way: in section 2 we introduce our system M-Id, section3 will present an overview of the electronic identity and what their possibilities and limitations are, in section 4 we look at the E-Government development and barriers, in section 5 we describe and discuss the proposed system using NFC enabled Smartphone, we finally conclude the paper in section 6.

2. OVERVIEW OF THE M-ID SYSTEM
This section presents the proposed identification solution using NFC enabled mobile devices. M-Id is a development of eId card system designed to identify citizens to different services. M-Id enables legally binding identification of users and authentication for banking services, payment confirmation, corporate services, access services, and government services. The authors of [5] propose an NFC mobile payment application based on the authentication and identification capabilities of the SIM card in mobile phones, which is very similar to Google Wallet, the application is not limited to payments it can also be used for identification. Our system is based on a specialized mobile-ID SIM card which the customer must request from the mobile phone operator(figure1). The certificates are stored on the mobile SIM card along with the application for identification, authentication and signing. Mobile-ID is a service that allows a client to use a mobile phone as a form of secure electronic ID.

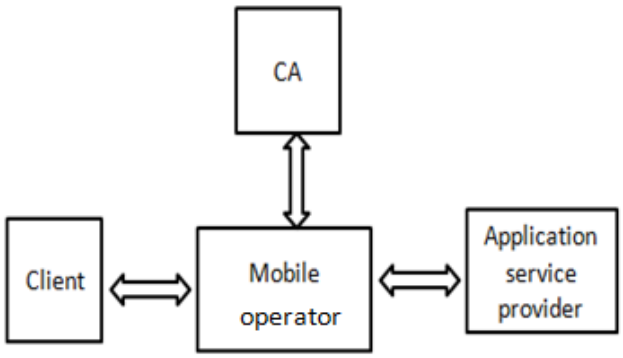

Fig1: The M-Id system

Thanks to the SIM card the system must fulfils three functions: identification, authentication, and signature. The first function of any ID card is to identify the holder. The mobile ID card contains exactly the same information as the traditional identity card but now the information is contained on the SIM card. M-ID thus enables two different levels of identification:

- Visual face-to-face identification: thanks to the information visible on the application interface (same as IDcard).

- Automatic identification: using data capture of the information stored on the SIM. This identification can be done remotely over the Internet or by contactless via NFC.

This identification (either visual or automatic) does not, however, guarantee that the holder is the person they claim to be. To verify this, authentication is required. The second function is the authentication of users. The SIM card in the mobile phone contain a digital authentication certificate that 'electronically' proves the identity of the user. To identify himself, the user places the phone in a NFC reader. Authentication offers an even higher level of security than identification because it requires the user to be in possession of PIN number. The third function is The electronic signature that has the same legal value as its paper equivalent. After having introduced the e-ID card into the reader, the citizen keys in the PIN which then generates a signature that is unique to the document. The SIM card contains personal information (name, surname, date of birth,...) and biometric data (photo and fingerprint) of a users, and cryptographic components : certificate , user signature..

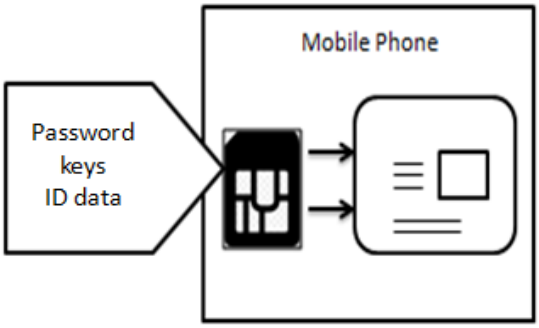

Fig 2: Overview of the system

2.1 E-Government on Smartphone

All the identity documents are owned by the government, and even often by one government agency[6]. And it seems like an impossible feat for agreeing on a specification for a government-wide credential which can be carry by a third-party token, such as a mobile phone. However, from the citizen's perspective, it is not preferable to have several smartcards in one wallet. Because People may leave home without their wallet, but they rarely forget their mobile phone. So having a copy of the identity card in the phone would allow more flexibility in the identification process. M-Id solution, need to be carried and deployed securely from the government server to the phone, and would require the a certification of the phone's secure element . In addition, secure handling of private data would need to be ensured by a Trusted Execution Environment on the mobile phone. since the mobile phone is often more preferable to use than a physical wallet The system could make life easier. To become a reality, the mobile phones should be with adequate security and the ability to communicate with contactless ID cards and passport readers. This is the area of NFC-enabled phones that support contactless communication protocols to emulate transit cards, payment cards, and even government ID cards. The following types of services might see an immediate benefit from supporting mobile ID:

- Government services that require formal identification of citizens.
- Services that must allow citizens to exercise their right to access personal information, may want to let citizens access their data online, but they have to identify the requestor.
- Companies that are required to record the identities of their clients, such as banks or telecommunications operators.

3. ELECTRONIC IDENTITY CARD

The electronic identity (eID) is used in many nations such as Danmark[7] Germany[8], Spain[9] and Turkey[10]; The electronic identity card is a physical card with smart card capabilities, used to authenticate users electronically. The majority of eID cards have a contact based interface(ISO 7816-3) similar to secure element. However some utilize a contactless interface(ISO14443). The smart card contains sensitive information, biometric data is protected using PKI, and biometric templates for authentication. To protect the private of the eID holder the biometric templates are not released until mutual authentication is performed. For authentication the eID card can be used with or without biometric data depending on the authentication policy of the given service, however for high level security all three authentication factors are used, biometric templates, pin-code and the card itself. The card is compatible with most smart card readers, however it requires a specialized device known as a Card Access Device (CAD) to use the biometric authentication. The three levels of authentication achieves very high levels of security and is difficult to compromise, since the authentication process itself is done online with an authentication server[11]. The eID has great potential and is definitely very secure which is naturally a requirement for a device which is supposed to be used with e-Government applications. The fact that most eID use a contact based interface if from a security perspective a safer alternative to contactless interface, as it is far more difficult to eavesdrop a contact interface as it requires physical tampering with the card readers.

4. THE M-ID APPLICATION

The M-ID must be able to confirm the identity of citizens and allow them to access different administrations, establishments and services. The M-ID provides the clients authentication, and it consists of two artifacts: a certificate and a signed ID image. Both artifact are protected by a digital signature which ensures the integrity and authenticity of the artifacts. It runs the M-ID application which is capable of interacting with other NFC enabled devices (figure3). The M-ID is stored on the phone allowing for offline authentication. The actors of the application M-ID are the users (citizens), the government which provides interfaces and servers to facilitates M-ID, and the third party which is presented with the access control.

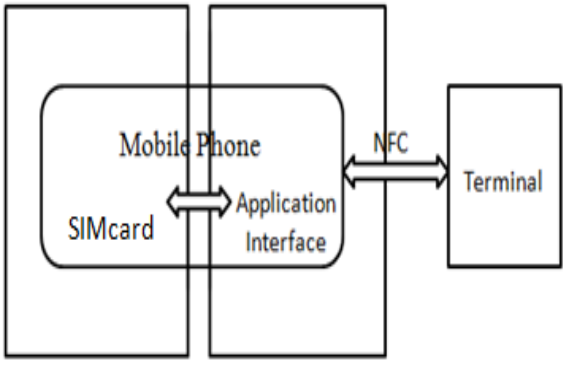

Fig3: System Architecture

The proposed application is based on a client-server model(figure(4). The application architecture is divided in two different type of entities: control app entities and NFC entities.

The communication between the server App and the client App is done by NFC links. Both the client App and the server App are divided into two different types of entities, namely NFC entities and App entities. The first type of entities makes possible the NFC peer-to peer connections and the App entities control the encryption/decryption involved in the authentication procedure at application level.

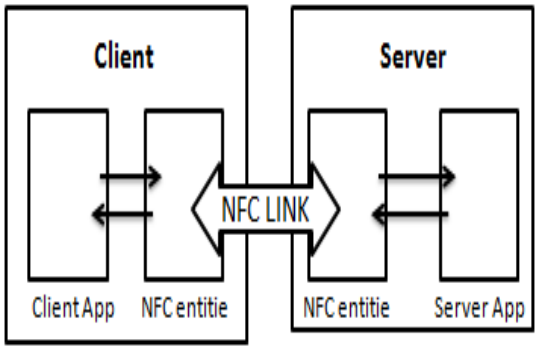

Fig4: Application Architecture

5. CONCLUSION

In this paper we have presented a new secure access system based on the mobile Id card and NFC. The immediate benefits of the M-Id system will be a reduction in the expenses paid by the government for creating and distributing plastic eID cards containing RFID chips and magnetic stripes. The novel system enables the exchange of crucial information through secure wireless peer-to-peer communications. In the next study we will present the simulation part of the system enables the exchange of crucial information through secure wireless peer-to-peer communications.

6. REFERENCES

[1] C.Mulliner; 2009.Vulnerability analysis and attacks on NFC-enabled mobile phones. Availability, Reliability and Security; ARES '09. International Conference.

[2] http://www.aptiqmobile.com/AreYouReady/Index.html

[3] NFC World “Emirates government begins NFC national id project”. 2012. [Online]: http://www.nfcworld.com/2012/04/11/315015/emirates-government-begins-nfc-national-id-project/

[4] T. Abe, H. Itoh, K. Takahashi. 2007.Implementing Identity Provider on Mobile Phone; Digital Identity Management; page 46-52. ACM.

[5] W. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, & J. Chiu. 2010. NFC Mobile Transactions and Authentication Based on GSM Network. Near Field Communication (NFC); Second International Workshop on doi: 10.1109/NFC.

[6] Å.Grönlund , T. A. Horan; 2005INTRODUCING e-GOV: HISTORY, DEFINITIONS, AND ISSUES; Academic Journal.

[7] N. Triantafyllidis, C. Jacoby. 2008. eID/Authentication/Digital signatures in Denmark.

[8] D.Hühnlein, D.Petrautzki, J.Schmölz, TobiasWich , M. Horsch, T.Wieland , J.Eichholz, A.Wiesmaier, J.Braun, F. Feldmann, SimonPotzernheim, Jörg Schwenk., C.Kahlo, A.Kühne ; HeikoVeit. 2012. On the design and implementation of the Open eCard App.

[9] A.Heichlinger, P. Gallego; 2010. A new e-ID card and online authentication in Spain; dentity in the Information Society.

[10] Mutlugün, Adalier . 2009.Turkish national electronic identity card.

[11] A.Poller, U. Waldmann, S. Vowé, S. Turpe. 2011. Electronic Identity Cards for User Authentication – Promise and Practice; IEEE.