Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 21 (2013) 91 – 98

Procedia Computer Science

The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013)

Authentication Systems Using ID Cards over NFC Links: the Spanish Experience using DNIe

J. M. León-Coca[a], D. G. Reina[a], S. L. Toral[a], F. Barrero[a], N. Bessis[b] a*

[a]*University of Seville, Seville, Spain*

[b]*University of Derbi, Derbi, UK*

Abstract

The personal identification in mobile scenarios has attracted a lot of attention in the last few years due to the emergence of new communications paradigms that enable the establishment of ad hoc communications. These communications must be carried out in a secure way since they can be involved in applications such as payments and access systems. Consequently, new secure systems should be proposed for managing security in such complex, mobile and variable conditions. This paper proposes a new authentication system based on the Spanish ID card and the wireless NFC (Near Field Communication) technology. It uses cryptography techniques and authentication certificates to establish secure communications between two interlocutors. The proposed network oriented architecture enables the proposed authentication system to operate in both local and remote modes.

Selection and peer-review under responsibility of Elhadi M. Shakshuki

Keywords: Authentication, PKI, RSA, NFC

1. Introduction

New security threats have emerged due to the recent growth of mobile computing and the intensive use of Internet. The birth of new communication paradigms like the Internet of things (IoT) envision a world full of connected devices capable of exchanging information through Internet. The communications among such mobile devices must be carried out in a secure way so the identification of the interlocutors taking part in any communication is required. This identification process in existing networks is a complex mechanism that introduces new secure systems for authenticating interlocutors in mobile

* Corresponding author. Tel.: +44 (0) 1332 592108; fax: +44(0) 1332 597741.
E-mail address: N.Bessis@derby.ac.uk.

1877-0509 © 2013 The Authors. Published by Elsevier B.V. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of Elhadi M. Shakshuki
doi:10.1016/j.procs.2013.09.014

scenarios. National Governments have joined this scenario during the last decade, modifying the existing identity (ID) cards to include the electronic identification of citizens, eID cards.

This is the case in Spain, where people are normally indentified by their personal ID cards. These cards are currently issued by the national government, containing electronic personal information that can be used for identification purposes. The Spanish government is currently promoting the use of the eID cards distributing the API for developing new services based on it [1] and offering free training courses [2]. In addition to these resources, it can also be found a complete Public-Key Infrastructure (PKI) based on the Spanish eID card and the suitable management of digital certificates included in them. This infrastructure is supervised by the *Dirección General de la Policía*, DGP from now on, which is part of the *Ministry of Interior* [3]. With regard to developers, it provides a low cost method for personal authentication without any additional maintenance. It is worth pointing out that the electronic advanced signature is considered like the handwritten signature by the Spanish law. This electronic personal certificate is normally validated using offline methods that require the public certificate of the certification authority [4]. Also, services as validation authority are offered through the Online Certificate Status Protocol (OCSP) [5] that improves the process with an updated certificate revocation list.

There are multiple devices and authentication systems which can take advantage of this infrastructure like cash machines, digital television receivers, mobile adapters, etc., but time constrains normally limit its use. Short range wireless technologies can facilitate the use, enabling the establishment of ad hoc communications between two interlocutors. Among them, NFC has drawn a lot of attention in the last decade due to their suitable features in secure access applications. In this paper, the Spanish eID card and the NFC technology are joined to develop a new security access system, where the NFC technology is used as an enabling technology to establish wireless ad hoc communications. The proposed system uses cryptography techniques to establish a secure communication link and relies on the Spanish PKI to get the personal authentication.

The paper is organized as follows. Section II describes the PKI concept and some interesting cryptographic methods. Section III analyzes the Spanish eID card, while the NFC technology is studied in section IV. The presented application that combines NFC technology and the Spanish eID card is shown in section V. Finally, some conclusions are drawn in the last section of the paper.

2. Public-Key Infrastructure (PKI)

PKI is a security infrastructure that incorporates hardware, software, standards, and policies to create a framework for securing transmissions, verifying and validating identities, and ensuring the integrity and source of data through the use of asymmetric encryption and digital certificates [6]. It was proposed to solve the problems with the secure key exchange arisen with the use of symmetric key algorithms [7][8][9] and in addition, the "man-in-the-middle" (MITM) [10] vulnerability exhibited by the public-key cryptosystems [11]. The PKI concept was included in the X.509 ITU-T recommendation [12] which suggests the following characters [13]: 1) Certificate Authority (CA), 2) a security policy, 3) Registration Authority (RA), 4) certificate repository and distribution system, and 5) PKI-enabled applications. Basically, it is based on the suitable management of digital certificates. Digital certificates are issued by CAs and they are mainly composed of a private key, a public key and a document created following the X.509 standard, which is also known as X.509 certificate, and is signed previously by a CA. The veracity of certificating relies on the CA, if the CA and its methods can be trusted, then the certificate will be also trusted. It is interesting to know the content of a X.509 certificate, illustrated in the Figure 1.

Following the aforementioned characters of a PKI infraestructure are particularized in the Spanish case: the DGP acts as a root the CAs, its certificates are auto-signed [14] with a validity of thirty years, and it issues the certificates of the subordinated CAs with a validity of fifteen years. Currently, there are three subordinates CAs, their main function is to issue the digital certificates of the Spanish eIDs. The security policy can be found in [3] where is explained the concerned activities with the digital certificates during their lifetime as a guide in the relationship between the users and the Spanish eID card. All the issue offices of the National Identity Document serve as a RA and distribution system offering to citizens their owns PINs and managing their certificates. The validation authority is the *Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda* (FNMT) acting as certificate repository and as a PKI-enabled application providing an universal and redundant service of validation. Finally, all the applications, including the one proposed in this paper, that make use of this PKI can be considerated as PKI-enabled applications.

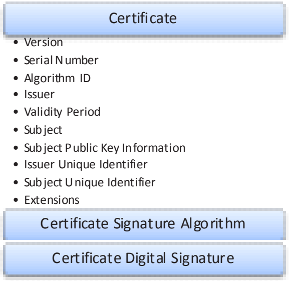
Certificate
• Version
• Serial Number
• Algorithm ID
• Issuer
• Validity Period
• Subject
• Subject Public Key Information
• Issuer Unique Identifier
• Subject Unique Identifier
• Extensions
Certificate Signature Algorithm
Certificate Digital Signature

Fig. 1. X.509 Certificate

3. Spanish eID (DNIe)

The Spanish eID, now on DNIe, is the official identification card used in Spain which is compulsory for citizens over fourteen years old residing in Spain or immigrants moved to Spain who have been living in Spain for more than six months. This card is a personal and non-transferrable document issued by the Ministry of the *Interior*. The Figure 2 shows the Spanish DNIe. The DNIe will be described discerning between its physical characteristics and the digital information contained in its chip.

Physically, DNIe is a polycarbonate card with the same dimensions of credit cards. In fact, it follows the ISO 7816 standard as a smart card [15]. It includes personalized information such as a photograph, and the personal signature, among other personal information. This information is written in OCR-B format [16] in order to facilitate the optical character recognition. In addition, changeable laser image techniques are used to print the expedition date and the holder's initials. It is important to highlight at this point that several security elements are included in the DNIe. These elements are classified according to their perception capabilities:

- First level (user perception): Holograms, kinegrams, iridiscences, OVI inks, multiple laser image, tactile word, superficial structures.
- Second level (perception using devices): reactive UV inks, microwriting, ghost photograph, security background, fluorescent inks.
- Third level (laboratory perception): Biometric comparison.

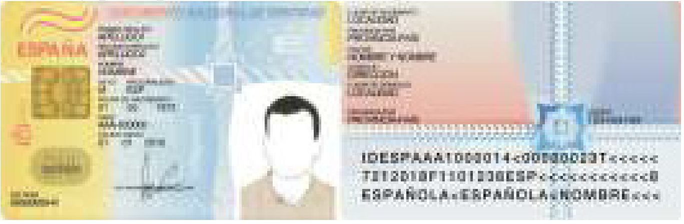
ESPAÑA
IDESPAAA1000014<00000023T<<<<<
7212018F1101238ESP<<<<<<<<<<<8
ESPAÑOLA<ESPAÑOLA<<NOMBRE<<<<

Fig. 2. (a) front DNIe; (b) back DNIe

From the point of view of the digital data included inside DNIe chip, the information is divided into three different security levels which are in read-only access. These levels are:

- Public zone (without restricted access): CA intermediate issuing certificate, holder public keys, component certificate.
- Private zone (access with PIN): Holder signature and authentication X.509v3 certificates and holder private keys.
- Security zone (only accessible through police equipment): Electronic information which is the same than that physically written, biometric data, and the device serial number.

The DNIe is considered a Secure Signature Creation Device (SSCD) according to the Common Criteria EAL 4+ in the protection profile CWA 14169 [17] certified by the ETSI, the RFC 3739 and the European directive 99/93/EC [18].

Now we are going to focus on the holder signature certificate since it is used in the proposed application. The purpose of the signature certificate is to allow the citizens to have the possibility of digitally signing transactions and documents, guaranteeing both integrity and authorship. To get the signature certificate is necessary to insert the holder PIN over a trusted channel [17] with the SSCD. Each signed task has to be authorized by the DNIe holder since the advanced electronic signature is compared to the legal hand signature [19], [20]. Notice that the electronic advance signature has the same validity of the legal hand signature. Therefore any application must always notify a user what and when a document will be signed. The certificate included in the DNIe follows the standard X.509v3.

4. Near Field Communication (NFC)

NFC is a set of standards for short-range communications. NFC has attracted much of attention during the last few years and it is estimated that by 2015 today's market value will be increased by eight times [21]. As a rule, in NFC communications there is an initiator and a target device. Both devices can operate in passive or active modes. In the active mode the devices must be supplied by batteries. In the passive mode, the target device uses the energy transported by the electromagnetic waves to send back a response to the initiator. The number of applications in which NFC technology is used is large, including applications such as secure payment tools, access management, and retailing industry among others. Furthermore, NFC is envisioned as an enabling technology for the Internet of Things [22].

In this paper we focus on peer-to-peer communications over NFC links. In peer-to-peer communications nodes work in the active mode. Figure 3 represents the NFC stack used in the proposed application to establish peer-to-peer communications between two NFC devices (NFC dongles). The Logical Link Control Protocol (LLCP) allows two types of peer-to-peer communications, connection-oriented transport and connectionless transport. While in the former the transmissions are guaranteed via ACKs, in the latter the transmissions are not guaranteed. For this reason, the connection-oriented transport has been chosen.

The nfcpy API has been used to code the programs responsible for managing the NFC communications [23]. This API, which is written in Python, allows users to define LLCP sockets with connection-oriented transport.

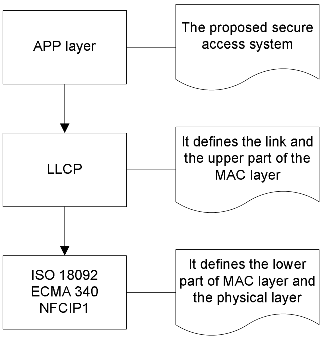
APP layer
The proposed secure access system
LLCP
It defines the link and the upper part of the MAC layer
ISO 18092
ECMA 340
NFCIP1
It defines the lower part of MAC layer and the physical layer

Fig. 3. NFC stack

5. Application: Secure Access System

In this paper we propose an application which identifies people carrying a DNIe using NFC links. The authentication is possible through the X.509 certificates included inside the DNIe. The proposed application enables the authentication and non-repudiation of the DNIe holder at the access moment thanks to the advance electronic signature. In addition, NFC links are used to exchange the application data through peer-to-peer ad hoc communications.

5.1 Application Architecture

The proposed application is based on a client-server model [24], see Fig. 4 (client APP-Server APP). While the server APP is responsible for granting the access, the client APP has a DNIe attached as a local resource. The communication between the server APP and the client APP was done by NFC links using LLCP protocol. Both the client APP and the server APP have been 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. Both entities communicate with each other through TCP/IP sockets.

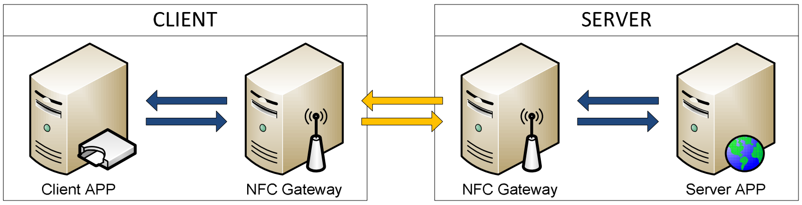

Fig. 4. Network Oriented Architecture

The NFC gateways entities were programming in python using the NFCpy API [23] and the LLCP protocol, which provides a mechanism to establish peer-to-peer connections between two NFC devices. The NFC entities are in charge of exchanging the information needed by the authentication procedure. The NFC entities also follow a client/server architecture based on LLCP sockets. While the initiator acts as a server NFC, the target functions as a client NFC.

The client and server applications were programmed in JAVA using the Spanish Government JAVA controller for the DNIe [1] which provides an easy access to the DNIe resources. These entities manage the authentication process [25] and implement a high level encryption to allow a secure connection among the server and the client.

This network oriented architecture solves the different programming languages used by APIs (java and python) and provides the capability of running the application in both local and remote modes. On one hand, the local mode consists of running the client/server entities configured with the localhost IP address. On the other hand, in the remote mode, both client/server entities are configured with their actual IPs addresses that paired the different entities because the NFC devices are not connected to the same computers in which the client APP and server APP are running, see Figure 4.

5.2 Communication among Entities

A new protocol was created to communicate the entities both NFC and the APP entities. It was called MAP-b64 (Standing for Mark-up ACE-Ti Protocol base64), which consists of a serial of messages used to establish or disconnect the communications and also as a method to send the information codified in base64. All the messages are sent between the marks '<' and '>'. If there is an error or simply the communication is successfully finished, the two escape characters <*> and <#> (see Figure 5), which are not included in the base64 dictionary, are used to close the communication or to report the occurred error.

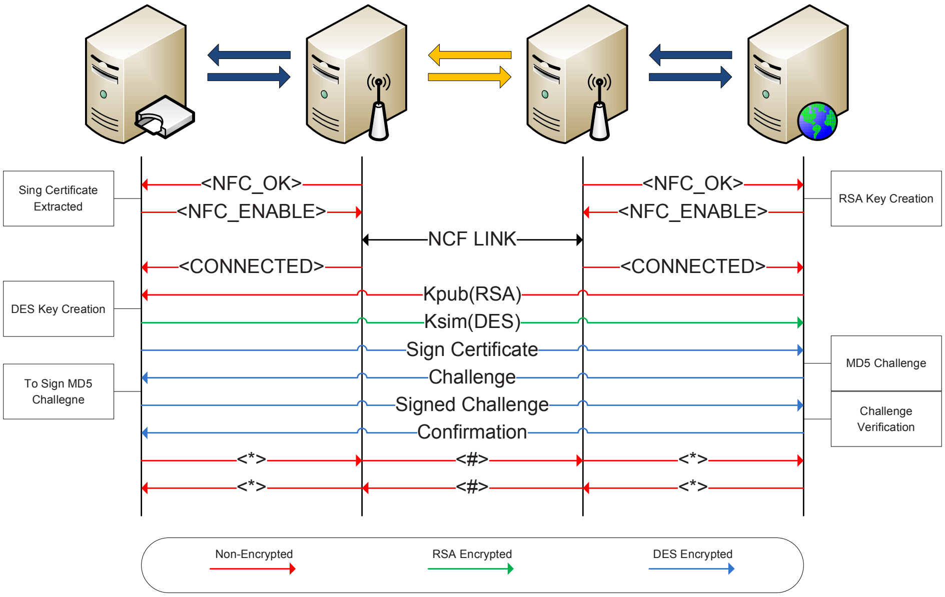

Fig. 5. Message exchange in the secure access system

The above Figure 5 illustrates the application functionality. It begins with establishing a communication between both APP entities and NFC entities, starting from client APP and server APP. The next step is the extraction of the signed certificate from the DNIe in the client APP side. On the other side, in the server APP, one pair of keys (public/private) is created to prepare a RSA encrypt process. Both, the client APP and the server APP are ready to try to connect to the paired NFC entities. The connection is established when the devices get closer. Then the server APP sends its public key and the client APP creates a symmetric DES [7] session key that will be sent to the server APP encrypted using its public key. As a result, a secure communication path between the server APP and the client APP is achieved. After reaching this point, all the information will be encrypted through a DES encryption. The following step is to start the authentication process which is composed of the following tasks 1) getting the signed certificate, 2) sending a single per session MD5 [26] hash challenge, 3) the sign of the challenge and the challenge validation. If the mentioned tasks are correctly accomplished, the server will grants or refuses the access to the system.

6. Conclusions

In this paper we have presented a new secure access system based on the Spanish DNIe and NFC. The novel system enables the exchange of crucial information through secure wireless peer-to-peer communications. The application architecture has been divided into two different types of entities, namely control APP entities and NFC entities. The former entities are based on a server-client architecture and they manage the security mechanisms used to safely exchange the data information such as the RSA encryption procedure and the DES session. In addition, they are in charge of the authentication procedure by using the certificate included in the Spanish DNIe. The NFC entities are responsible for establishing peer-to-peer communications between two NFC devices. The NFC entities perform as a wireless bridge to connect the control entities. Since the communication among entities is based on TCP/IP sockets, the proposed system can operate in both local and remote modes. In future works, this proposal will be adapted to new mobile applications in which the personal authentication is crucial. In addition, other wireless technologies like Bluetooth will be used instead of the NFC technology.

Acknowledgements

This work was supported in part by the University of Seville under the PhD grant PIF (Personal Investigador en Formación) of Daniel Gutiérrez Reina, and it has been developed in the framework of the ONLINE project (TSI-020100-2011-42) partially financed by the Ministry of *Industria, Turismo y Comercio* and FEDER in the AVANZA I+D program through the participation of ISOIN Company.

References

[1] Available at: http://zonatic.usatudni.es/aplicaciones/controlador-java-dnie.html

[2] Instituto Nacional de Tecnologías de la comunicación (INTECO). Formación DNIe. 2013. Available at http://www.inteco.es/Formacion/

[3] Dirección General de la Policía (Ministry of Interior). Infraestructura de Clave Pública DNIe. 2013. Available at: http://www.dnielectronico.es/PDFs/politicas_de_certificacion.pdf

[4] R. Housley, W. Ford, W. Polk, D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Technical report, RFC 2459:1999

[5] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Technical report, RFC 2560:1999

[6] Elias G. Carayannis, Eric Turner. Innovation diffusion and technology acceptance: The case of PKI technology, Technovation, 2006;26:847-855

[7] National Institute of Standard and Technology. Data Encryption Standard (DES) http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[8] X. Lai and J. Massey "A proposal for a new block encryption standard", Proceedings, Eurocrypt , 1990

[9] National Institute of Standard and Technology. Advanced Encryption Standard (AES) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[10] P. Burkholder. SSL man-in-the-middle attacks. SANS Reading Room; 2002

[11] Stacy Prowell, Rob Kraus, Mike Borkin, CHAPTER 6 - Man-in-the-Middle, Seven Deadliest Network Attacks, Syngress.2010:101-120

[12] International Telecommunication Union (ITU-T). X.509 Recommendation: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 2012.

[13] Ray Hunt, Technological infrastructure for PKI and digital certification, Computer Communications 2001;24:1460-1471

[14] Selwyn Russell, Ed Dawson, Eiji Okamoto, Javier Lopez, Virtual certificates and synthetic certificates: new paradigms for improving public key validation, Computer Communications, 2003, 26:1826-1838.

[15] International Standards Organization. ISO 7816 - Identification cards - Integrated circuit cards. 2011

[16] International Standards Organization. ISO 1073-2 - Alphanumeric character sets for optical recognition. 1976

[17] European Committee for Standarization (CEN). CEN Workshop Agreement (CWA) 14169. Secure signature-creation devices "EAL 4+" 2004

[18] Ministry of Industria, Energía y Turismo. Online Formation Platform. http://zonatic.usatudni.es/

[19] Jefatura del Estado (Spanish Government). Ley 59/2003, de 19 de diciembre, de firma electrónica. 2003

[20] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[21] Available at: http://www.abiresearch.com/research/1003525-Near+Field+Communications+NFC

[22] Reina D.G, Toral S. L, Barrero F, Bessis N, and Asimakopoulou. E. The role of ad hoc networks in the internet of things. Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence, Springer Berlin Heidelberg, 2013, pp. 89-113

[23] Avaialable at https://launchpad.net/nfcpy

[24] Jürgen Nehmer, Friedemann Mattern, Framework for the organization of cooperative services in distributed client-server systems, Computer Communications, 1992;15:261-269

[25] J. Franks, P.Hallam-Baker, J.Hostetler, S.Lawrence, P.Leach, A. Luotonen, L.Stewart. HTTP authentication: Basic and digest access authentication, Technical report, RFC 2617:1999

[26] R.L. Rivest, The MD5 Message-Digest Algorithm, Internet Activities Board, Technical report, RFC 1321:1992