



Repositorio Institucional de la Universidad Autónoma de Madrid

<https://repositorio.uam.es>

Esta es la **versión de autor** de la comunicación de congreso publicada en:
This is an **author produced version** of a paper published in:

International Joint Conference: CISIS'15 and ICEUTE'15. Advances in
Intelligent Systems and Computing, Volumen 369. Springer, 2015. 437-446

DOI: http://dx.doi.org/10.1007/978-3-319-19713-5_37

Copyright: © 2015 Springer International Publishing Switzerland

El acceso a la versión del editor puede requerir la suscripción del recurso
Access to the published version may require subscription

Using smart cards for authenticating in public services: A comparative study

D. Arroyo Guardado¹, V. Gayoso Martínez², L. Hernández Encinas², and
A. Martín Muñoz²

¹ Grupo de Neurocomputación Biológica, Departamento de Ingeniería Informática,
Escuela Politécnica Superior, Universidad Autónoma de Madrid
`david.arroyo@uam.es`

² Institute of Physical and Information Technologies (ITEFI)
Spanish National Research Council (CSIC), Madrid, Spain
`{victor.gayoso,luis,agustin}@iec.csic.es`

Abstract. Smart cards are well-known tamper-resistant devices, and as such they represent an excellent platform for implementing strong authentication. Many services requesting high levels of security rely on smart cards, which provide a convenient security token due to their portability. This contribution analyses two Spanish smart card deployments intended to be used for accessing eGovernment services, comparing their respective contents and capabilities.

Keywords: Cryptography, Digital signature, Electronic prescription, Smart cards

1 Introduction

Secure electronic identification is an important enabler of data protection and the prevention of online fraud. These aspects have a great importance in areas such as eGovernment, which consists of the digital interactions between governments, citizens, public agencies, and employees. In this scenario, the European Commission's eGovernment Action Plan 2011-2015 supports the provision of a new generation of eGovernment services, as well as the strengthening of services already deployed [1].

As a measure of its importance, only in Spain more than 480 million administrative procedures were conducted by citizens and companies with the central government in 2013, of which over 367 million (76.5%) were conducted electronically and over 112 million (23.5%) by other means. For enterprises, 94% of administrative procedures were done electronically and for citizens 65% [2]. Among the services for citizens most widely used in Spain we can find those related to income taxes (declarations, notifications of assessment, etc.), social security benefits (unemployment, pensions, etc.), the request of personal documents (passports, driving licences, etc.), and health related services (appointments for hospitals, etc.) [2].

This contribution analyses two smart card deployments for the authentication of users in public services, comparing their respective characteristics and capabilities: the Spanish electronic identity card (known as DNIE, *Documento Nacional de Identidad electrónico*), and the smart card delivered to part of the medical doctors working at the Community of Madrid for the electronic prescription service, which in this contribution will be referred to as the EPSC (Electronic Prescription Smart Card).

The rest of this paper is organized as follows: Section 2 provides a brief introduction to smart cards. Section 3 shows the details of the DNIE. In Section 4, the main features of the EPSC are included. Section 5 offers a comparison of both smart cards. Finally, our conclusions are presented in Section 6.

2 Smart cards

A smart card is a plastic card with an embedded chip that controls the access to the stored data. The two most widespread communication models for smart cards are the byte-oriented, half duplex transmission protocol T=0 and the block-oriented, half duplex protocol T=1, both defined in ISO/IEC 7816-3 [3]. The T=1 protocol is newer, and implements error detection capabilities.

The elements known as APDU (Application Protocol Data Unit), built according to the ISO/IEC 7816-3 [3] and 7816-4 [4] specifications, are the data packets exchanged between the external application and the card by means of a smart card reader. The card operating system is responsible for analysing any incoming APDU and redirecting it to the application it is intended for. The operating system is also responsible for retrieving the response data from the card application and submitting it to the external application using the card reader.

There are two types of APDUs: command and response. Figure 1 shows the format of command APDUs, which consist of a header and optionally a body with the following elements:

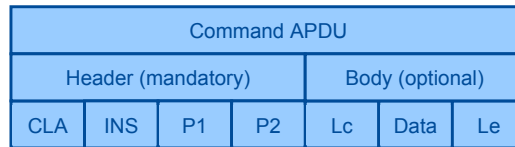


Fig. 1: Command APDU

- CLA (1 byte): Command class.
- INS (1 byte): Specific instruction within the class.
- P1 (1 byte): First parameter associated to the instruction. It can be used to give more information about the instruction, or as input data.
- P2 (1 byte): Second parameter associated to the instruction. As in the previous case, it can be used to give more information about the instruction, or as input data.

- Lc (1 byte, optional): Number of bytes in the data field of the command. Since its highest value is 0xFF, the maximum data length is 255 bytes, although some cards allow to send 256 bytes using the value 0x00.
- Data (variable size, optional): Information to be processed by the applet.
- Le (1 byte, optional): Maximum number of bytes to be included in the data field of the response APDU.

In comparison, the format of any response APDU is simpler (see Figure 2), as it only includes the following items:

Response APDU		
Body (optional)	Result (mandatory)	
Data	SW1	SW2

Fig. 2: Response APDU

- Data (variable length, optional): Information returned by the card application.
- SW1 (1 byte): First status byte, which provides general information about the result of the command execution.
- SW2 (1 byte): Second status byte.

Following the ISO/IEC 7816 notation, the smart card file structure is represented by means of two types of elements: DF (Dedicated File) and EF (Elementary File). While DFs can be interpreted as directories or folders of a standard file system, EFs can be considered to be data files, belonging either to the operating system or to other smart card applications.

3 DNIE

The DNIE is a T=0 smart card that allows to certify the identity of the DNIE holder and to digitally sign documents using electronic signature protocols with the same legal validity than a handwritten signature [5]. The DNIE is the soundest and preferred method to prove one's own identity in any act with the Public Administration. Since it was started to be issued, more than 43 millions of DNIE cards have been delivered to citizens [6].

In January 2015, it was announced a new version of the DNIE, called DNIE 3.0, which incorporates an NFC (Near Field Communications) chip with the goal to facilitate its usage with smartphones and tablets, avoiding the limitation of delivering smart card readers to potential users.

Figure 3 (left) shows the file tree of the DNIE, where the Master File (typically represented as the DF 3F00) is the root directory of the file system.

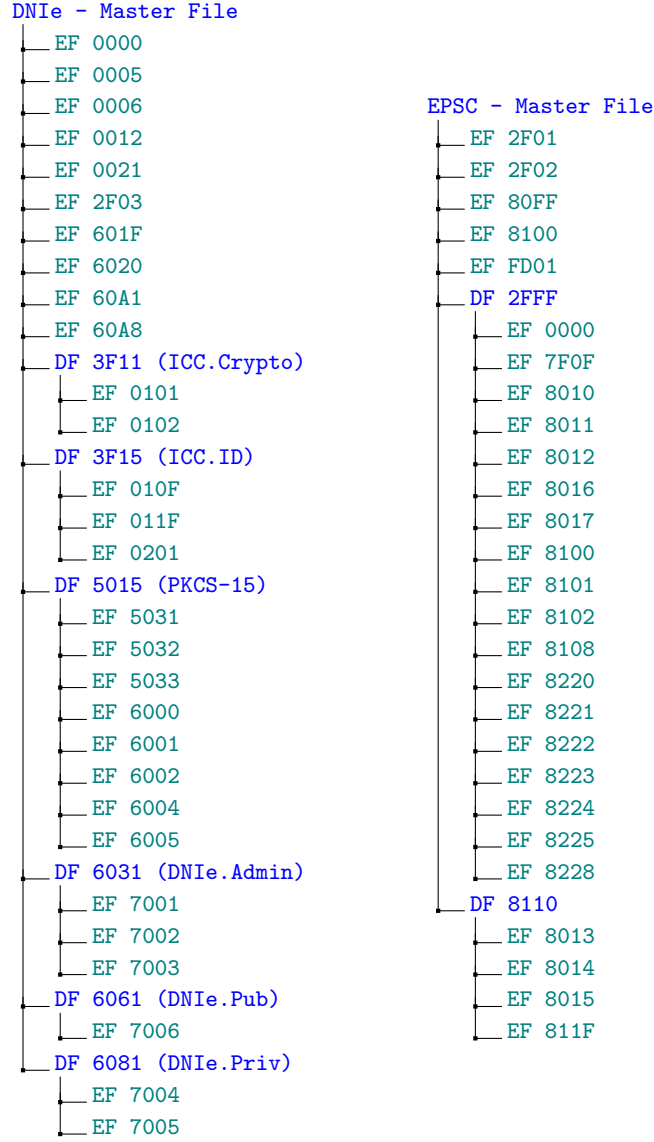


Fig. 3: File structure of the DNIE (left) and EPSC (right)

The information stored in the chip is divided into three areas with different access levels and security conditions [7–9]:

- Public area: Reading access without restrictions. It includes, among others, the following files:
 - EF 601F: X.509 component certificate (each DNIE has a different component certificate associated to the actual smart card), with an RSA public key of 1024 bits.
 - EF 6020: X.509 certificate of the component intermediate CA (Certification Authority), with an RSA public key of 1024 bits.
 - EF 7006: X.509 certificate of the DGP (*Dirección General de la Policía*) intermediate CA, with an RSA public key of 2048 bits.
- Private area: Reading access allowed after validation of the citizen’s PIN (Personal Identification Number) code. Some of the files included are the following:
 - EF 7004: X.509 user signing certificate with an RSA key of 2048 bits.
 - EF 7005: X.509 user authentication certificate with an RSA public key of 2048 bits.
- Security area: Reading access allowed only after biometric verification. In order to make this verification, the citizen must use the biometric devices located at the DNIE issuing offices. The files protected by this procedure are the following:
 - EF 7001: Citizen’s filiation data (name, surname, date of birth, etc.).
 - EF 7002: Digitized image of the citizen’s photograph.
 - EF 7003: Digitized image of the citizen’s handwritten signature.

Given that the DNIE is a device linked to the identity of the citizens, its security, both physical and electronic, is of paramount importance. In that sense, the DNIE is a SSCD (Secure Signature Creation Device) compliant with the European standard EN 14890-1 [10], which defines how to establish a communication between the SSCD and an external application. Because of that, the operating system of the DNIE subordinates the sending of certain APDUs (like the Verify PIN command) to the establishment of a secure channel [11].

In order to establish the secure channel, it is necessary to exchange the public keys of the card and the external application that wants to communicate with the DNIE. After those certificates are verified by both parties, they must perform a mutual authentication protocol, including a seed exchange for the derivation of the encryption and MAC (Message Authentication Code) session keys. Once the secure channel is established, any command must be protected before its transmission using the session keys.

In the descriptions that follow, the word *terminal* represents the pair formed by the software application that intends to communicate with the DNIE and the physical device where the application is executed, while the word *card* is used as an alternative to the terms DNIE and smart card.

The establishment of the secure channel consists of the following four phases:

1. Certificate exchange and verification:
Before starting the mutual authentication process, the terminal must send its authentication certificate to the card, so the DNIE can verify that the certificate is correct and has been properly signed by a trusted certification authority. If that is the case, the application will request the card component certificate in order to verify it. Once this exchange is completed, the application will have the public key and the certificate associated to the card, whilst the card will have obtained the public key and the certificate of the terminal.
2. Internal authentication:
In this phase, the terminal must request the card to perform a valid authentication. In order to do this, the terminal must generate a random number that is sent to the card as a challenge. The card uses this value to generate in turn its contribution to the session key creation process. If the terminal is able to recover that value, this means that the data provided by the card was valid and that the card has been successfully authenticated.
3. External authentication:
After the two previous phases, the terminal has identified the card as a valid DNIE. In order to complete the mutual authentication procedure, it is necessary to perform now the external authentication process, so the terminal is authenticated by the card, following a process similar to that of the previous phase.
4. Session key generation:
The last step consists in calculating the encryption and MAC keys that will be used in the communication through the secure channel.

4 Electronic Prescription Smart Card

EPS (Electronic Prescribing and Dispensing) is the term that identifies the system and processes that allow all the stages of the prescribing, supply of medicine, and claiming process to be completed electronically, providing an alternative to the typical paper based prescription system in public health environments.

EPS enables prescribers (mainly medical doctors) to create, sign, and send prescriptions electronically to a dispenser (such as a pharmacy) of the patient's choice or to a central server, from where they can be electronically retrieved by any dispenser. This makes the prescribing and dispensing process more efficient and convenient both for patients and the medical staff. EPS is a key initiative currently being implemented or already deployed in many countries (e.g. United Kingdom [12], Australia [13], etc.), and the European Union is focusing now in developing the interoperability of electronic prescriptions [14].

In Spain, the electronic prescription system being rolled out is not yet completed. As of December 2014, 89,58% of general health centers, 52,56% of local clinics, 66,21% of specialized centers, and 89,35% of pharmacies were already working with the new system nationwide, though the figures vary a lot between Autonomous Communities [15] (for example, at the beginning of 2014 it was already implemented in Communities such as Andalucía or Galicia, while in other

Communities such as Murcia it is expected to be rolled out during 2015 [16]). In the Community of Madrid, where we have made our study, the new system started to work across all the region at the end of 2014 [17].

In the current phase of the EPS deployment in the Community of de Madrid, medical doctors sign the prescriptions electronically using their login credentials. However, in next phases this system is expected to be replaced by a strong authentication scheme based on smart cards, and with that goal medical doctors have received their own, individual smart cards. As mentioned in the Introduction, in this contribution we will refer to this smart card as EPSC, which is a T=1 smart card.

Figure 3 (right) shows the complete file structure of the EPSC. All the files included in the figure can be read without verifying the user's PIN. The most interesting files are the following ones:

- EF 2F02: It includes the serial number of the smart card.
- EF 8223: This file contains details about the user, mainly the name, surname, and NIF (*Número de Identificación Fiscal*, the identification number of each Spanish citizen consisting of a sequence of 8 digits and a letter associated with that sequence. The NIF is the identification number displayed at the DNIe).
- EF 8224: It includes details about the intermediate CA.
- EF 8228: This file stores all the elements in the certificate chain up to the user's certificate, as it is displayed in Figure 4. Camerfirma is a company participated by more than 85 spanish Chambers of Commerce [18], and that is part of Chambersign, a European organization that provides support to national Chambers of Commerce from a supranational standpoint [19]. All three certificates shown in Figure 4 are related to RSA keys of 2048 bits.

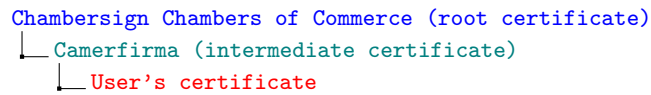


Fig. 4: EPSC certificate chain

Unlike the DNIe, it is not necessary to establish a secure channel before sending some APDUs like the Verify PIN command. Apart from that, it is interesting to point out that many files have an empty content (i.e., sequences of the byte 0x00). Presumably, the content of those files will be updated once the smart cards begin to be used.

Another difference between DNIe and EPSC is that, while the former follows the indications given by the PKCS #15 (Public-Key Cryptography Standards) standard [20], the file structure of the latter is not compliant with that specification.

5 Comparison

The chip mounted by the DNIE received the EAL5+ (Evaluation Assurance Level 5 augmented) accreditation in 2005 [21]. Besides, version 1.13 of the DNIE was evaluated as a smart card by the National Cryptologic Centre (CCN, *Centro Criptológico Nacional*), a government organization that belongs to the National Centre of Intelligence (CNI, *Centro Nacional de Inteligencia*), and obtained the EAL4+ (Evaluation Assurance Level 4 augmented) certification in 2007 [22].

The DNIE is equipped with several physical elements that allow to consider it a highly secure physical token. Among those items, we can highlight the following [7]: holograms, kinograms, optically variable inks, changeable laser images, surface relief structures, inks visible only under infrared or ultraviolet light, citizen's photography and handwritten signature engraved with laser, etc. In comparison, the EPSC is not equipped with the physical countermeasures just mentioned, and the details about its accreditation are not public.

Regarding their cryptographic capabilities, both the DNIE and EPSC contain the user's X.509 certificate as well as an associated 2048-bit RSA key pair intended for performing digital signatures.

However, the security of the DNIE is much more robust, as it only allows to send certain commands after establishing a secure channel which authenticates both the smart card and the software communicating with it. In the DNIE, the retrieval of certain elements, such as the user's certificates, can only be accomplished after correctly entering the PIN code. As the APDU containing the Verify PIN command can only be sent through the secure channel, an attacker cannot access the content of the user's certificates unless he knows the PIN code and establishes the secure channel. Another consequence of this scheme is that no attacker can block the PIN code of the DNIE without completing the process that sets up the secure channel.

In comparison, the EPSC allows to read all the files of its file system without the need of entering the PIN code, which allows an attacker to retrieve the user's certificate if he has access to the smart card. Besides, the attacker could block the PIN code, which would render the legitimate user unable to make signatures unless he was in possession of the PUK (Personal Unlocking Key) code.

Regarding the Spanish legislation associated to digital signatures, we remind the readers that the Law 59/2003 establishes the following concepts [5]:

- Electronic signature: It is the set of electronic data that can be utilized as a means of identifying the signing user.
- Advanced electronic signature: It is the electronic signature that allows the signing user to be identified. The signature must be created by methods that the signing user can keep under his exclusive control.
- Qualified electronic signature: It is the advanced electronic signature based on a qualified certificate and generated by a secure signature creation device.

Based on those definitions, the DNIE can be considered as a device that allows to generate qualified electronic signatures. The EPSC, unless fully accredited,

would have to be considered as a device allowing to generate only advanced electronic signatures which could not be used in another environments.

6 Conclusions

As described in the previous sections, the DNIE is a highly secure, certificated smart card that allows to generate qualified electronic signatures. Even though some technical information about the EPSC is not available to researchers, it can be considered a less robust authentication device.

If we take into account that the latest version of the DNIE includes support for NFC devices, it seems reasonable to suggest the use of the DNIE instead of the EPSC for the task of signing the electronic prescriptions. This decision would be doubly beneficial: on the one hand, it would allow to avoid the cost of purchasing the smart cards and delivering them to the medical doctors; on the other hand, it would allow doctors working with NFC-capable devices such as modern tablets and smartphones to avoid installing smart card readers, which additionally represent an avoidable cost for health centres that had not purchased them before.

Finally, from a standards perspective, the DNIE fully adapts to the PKCS #15 structure, which facilitates interoperability with future applications.

Acknowledgment

This work has been partially supported by Comunidad de Madrid (Spain) under the project S2013/ICE-3095-CM (CIBERDINE).

References

1. European Commission: European eGovernment Action Plan 2011-2015. (2011) <https://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015>.
2. European Commission: eGovernment in Spain. (2014) <https://joinup.ec.europa.eu/sites/default/files/41/be/69/eGov%20in%20ES%20-%20February%202014%20v.16.0.pdf>.
3. ISO/IEC: Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 7816-3, 3rd ed. (2006)
4. ISO/IEC: Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 7816-4, 3rd ed. (2013)
5. Fábrica Nacional de Moneda y Timbre: Electronic signature. <https://www.sede.fnmt.gob.es/en/normativa/firma-electronica>.
6. Dirección General de la Policía: Página oficial de la DGP - Notas de prensa. (2015) http://www.policia.es/prensa/20150112_1.html.

7. Espinosa García, J., Hernández Encinas, L., Queiruga Dios, A.: The new Spanish electronic identity card: DNI-e. In: Proceedings of the International Conference on Information Technologies (InfoTech'2007), volume I: Technological Aspects of the e-Governance and Data Protection. (2007) 77–82
8. Ministerio del Interior de España: Portal oficial sobre el DNI electrónico. (2013) <http://www.dnielectronico.es/>.
9. Gayoso Martínez, V., Hernández Encinas, L., Martín Muñoz, A.: La tarjeta de identidad española como método de autenticación en redes sociales. In: VII Congreso Iberoamericano de Seguridad Informática 2013 (CIBSI 2013). (2013) 32–44
10. CEN: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services. European Committee for Standardization. UNE-EN 14890-1. (2009) <http://www.cen.eu/cen/Sectors/TechnicalCommitteesWorkshops/CENTechnicalCommittees/Pages/Standards.aspx?param=6205&title=CEN\%2FTC+224>.
11. Ministerio del Interior de España: Documento Nacional de Identidad electrónico: Guía de referencia técnica. (2012)
12. Health and Social Care Information Centre: Electronic Prescription Service. (2015) <http://systems.hscic.gov.uk/eps>.
13. Department of Human Services: Electronic prescribing and dispensing of medicines. (2014) <http://www.medicareaustralia.gov.au/provider/pbs/pharmacists/dispense.jsp>.
14. eHealth Governance Initiative: Guidelines on ePrescription. (2014) <http://www.ehgi.eu/Lists/Posts/Attachments/15/eHealth%20Network%205%205BAthens%202014%5D%20Topic%206%20-%20Discussion%20Paper%20-%20Guidelines%20on%20ePrescription.pdf>.
15. Oficina para la Ejecución de la Reforma de la Administración: Informe de Progreso de la Comisión para la Reforma de las Administraciones Públicas. (2015) http://www.seap.minhap.gob.es/dms/es/areas/reforma_aapp/proceso/CORA-Informe-anual-de-progreso--Diciembre-2014/CORA-Informe%20anual%20de%20progreso.%20Diciembre%202014.pdf.
16. Sociedad Española de Farmacia Comunitaria: Estudio de implantación de la receta electrónica en España. (2014) http://www.farmaceticoscomunitarios.org/sites/default/files/wysiwyg/181_brizuelarodicioluis_recetaelectronica_recetaelectronica.pdf.
17. Gaceta Médica: Madrid culmina la implantación de la e-receta. (2015) <http://www.gacetamedica.com/noticias-medicina/articulo.aspx?idart=884387&idcat=797&tipo=2>.
18. Camerfirma: About us. (2015) <http://www.camerfirma.com/camerfirma/quienes-somos/>.
19. Chambersign: About us. (2015) <http://www.chambersign.com/about-us>.
20. ISO/IEC: Identification cards – Integrated circuit cards – Part 15: Cryptographic information application. International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 7816-15. (2004)
21. ANSSI: Produit certifié Critères Communs (réf: 2005/40). Agence Nationale de la Sécurité des Systèmes d'Information. (2005) http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cc/certificat_2005_40.html.
22. CCN: Informe de certificación INF-148. Centro Criptológico Nacional. (2007) http://www.dnielectronico.es/seccion_integradores/cc1_p.jpg.