http://dx.doi.org/10.1049/iet-ifs.2017.0299

# Security Assessment of the Spanish Contactless Identity Card

Ricardo J. Rodríguez[1,*], Juan Carlos Garcia-Escartin[2], Víctor Sánchez-Ballabriga[1]

[1]Dept. of Computer Science and Systems Engineering, University of Zaragoza, Spain
[2]Dept. de Teoría de la Señal y Comunicaciones e Ing. Telemática, University of Valladolid, Spain
[*]rjrodriguez@ieee.org

**Abstract:** The theft of personal information to assume the identity of a person is a common threat. Individual criminals, terrorists, or crime rings normally do it to commit fraud or other felonies. Recently, the Spanish identity card, which provides enough information to hire on-line products such as mortgages or loans, was updated to incorporate a Near Field Communication (NFC) chip as electronic passports do. This contactless interface brings a new attack vector for these criminals, who might take advantage of the RFID communication to secretly steal personal information. In this paper, we assess the security of contactless Spanish identity card against identity theft. In particular, we evaluated the resistance of one of the contactless access protocol against brute-force attacks and found that no defenses were incorporated. We suggest how to avoid brute-force attacks. Furthermore, we also analyzed the pseudo-random number generator within the card, which passed all performed tests with good results.

## 1. Introduction

Identity theft is defined as the theft of personal information, such as name, date of birth, etc. – that is, any data that allows a party to fake the identity of another party [24]. Each country defines different laws that protect their citizens from this kind of theft. For instance, the Spanish law punishes the use of personal information to fake the identity of an individual and perform actions on its behalf with up to three years of prison [2].

In Spain, this personal information is collected in the Spanish identification (ID) card, abbreviated as DNI (*Documento Nacional de Identidad*, in Spanish), which is issued to any Spanish citizen. Data contained on this card is, among others, the first name, the family names, the unique identification number of the citizen, and the birth date.

An identity theft is normally performed by an individual criminal, a terrorist, or a crime ring, who will take advantage of the identity to commit fraud or other felonies [42]. In Spain, data written on the DNI are enough to hire different on-line products (as telecommunication services, mortgages, or loans). Some reports quantified a total of 4.5 million of these cases in Spain, with an average fraud of 8000€ per case [15].

Some examples of felonies performed by criminals after the theft of Spanish ID cards are reported in [43]. For instance, during 2010 a Spanish male citizen repetitively stole DNIs from gym lockers to later obtain personal information (such as tax information) and then ask for credit cards and loans on behalf of victims. The DNI of a female citizen was stolen in Madrid subway, and then used by a convenience marriage mafia. Another Spanish male citizen went to Italian jail for 626 days after he sold his DNI, which was later used to check-in in Italian hotels by a Napolitan

mafia-related drug dealer.

Recently, the DNI card was updated to incorporate a Near Field Communication (NFC) chip, as electronic passports (e-passports, for short) do [5]. NFC is a bidirectional short-range (up to 10 cm) contactless communication technology operating in the 13.56 MHz band based on the ISO-14443 [22] and the Sony FeLiCa [25] Radio Frequency Identification (RFID) standards. NFC is vulnerable to multiple threats such as eavesdropping, data modification (i.e., alteration, insertion, or destruction), or relay attacks [18, 29, 40]. NFC is emerging in a wide range of applications, from ticketing, staff identification, or physical access control, to cashless payment, to name a few. Following this trend, to date, almost 300 different NFC-enabled phones are (or will be soon) available at the market [34]. Hence, the eruption of NFC-enabled phones (or devices) may bring criminals a new attack vector to these NFC-enabled ID cards, as DNI or e-passports.

In this paper, we performed an independent security assessment of the NFC-enabled DNI. In particular, we evaluated the possibility of stealing personal information from a Spanish citizen without his/her knowledge using NFC capabilities. Our experiments showed that, in general, the protocols used to communicate via contactless with a DNI are secure enough and well coded. However, we discovered that the DNI did not incorporate any mechanism to prevent (on-line) brute-force attacks. We also proposed a defense mechanism. Our findings were communicated to the Spanish National agency in charge of the Spanish ID card development, who acknowledged us by taking our defense proposal into consideration for future revisions.

This paper is organized as follows. Section 2 gives some background, in particular regarding the Spanish ID card and the ISO/IEC 14443 standard. Section 3 introduces the protocols used to communicate with NFC-enabled DNI (namely, the Basic Access Control and the Password Authenticated Connection Establishment protocols). Security assessment is detailed in Section 4. Section 5 reviews the related work. Finally, Section 6 concludes the paper.

## 2. Background

In this section, we first review the evolution of Spanish ID card. Then, we first briefly introduce the ISO/IEC 14443 standard [22] in which the latest version of electronic Spanish ID card relies on.

### *2.1. Spanish Identity Card*

The first Spanish ID card dates back to the first years after the Spanish Civil War, in 1941. On those dates, it was issued by local governments. Ten years later and after a national decree, the first DNI was issued to the Spanish general and dictator Francisco Franco Bahamonde. These ID cards where issued first to persons on probation and prisoners, then to frequent male travellers (due to their business or profession), and later to male population residing in cities with more than 100000 inhabitants. After that, it was issued to male population residing in cities within 25000 and 100000 inhabitants and then to frequent female travellers, and so on and so forth until reaching the whole of society.

In the following years, several revisions of the DNI were proposed, sometimes adding or removing personal data (civil status, blood type, and economic status were present during first versions, later removed). The first electronic DNI, named DNIe2.0, was issued in 2006. It incorporated an electronic chip and several physical security elements to prevent card forging. The electronic chip is a 32K STMicroelectronics ST19WL34. According to official documents [12], data within


(a) (b)

***Fig. 1.*** *(a) Front side and (b) reverse side of the Spanish contactless ID card (extracted from [13]).*

the chip is divided into three different zones: a *public zone*, which contains the intermediate CA certificate, Diffie-Hellman keys, and the X.509 certificate (read with no restrictions); a *private zone*, which contains the signature and authentication certificates of the citizen (only accessible through a PIN); and a *security zone*, which contains the citizen data (all data printed also on the front of DNI), facial picture, and the handwritten signature image (only accessible through special locations).

Recently, in 2015, the electronic DNI was improved by adding contactless capability into it. This revision was named as DNIe3.0. In particular, it adds a Near Field Communication (NFC) chip. Furthermore, it also adds new physical elements to make forging even harder. The chip is an Infineon Technologies SLE78CLFx408AP with 400K of capacity and 8KB of RAM [13]. This chip has successfully passed the Common Criteria EAL5+ certification. It supports several cryptographic algorithms, such as RSA (through a built-in RSA library following the PKCS#1 standard for key generation), SHA-256 hashing to validate authentication commands and certificate validation, and 3DES and AES symmetric-key algorithms. According to official documents [13], in this case data within the chip is divided into two different zones: a *public zone*, which contains the intermediate CA certificate, Diffie-Hellman keys, X.509 certificate, and the signature and authentication certificates of the citizen (read with no restrictions); and a *security zone*, which contains, as before, the citizen data (all data printed also on the front of DNI), facial picture, and the citizen's scanned handwritten signature (only accessible through special locations). Let us remark that we were able to access to the security zone without being in a special location, contrary to it was stated in the official documents. All those data are divided into four different data groups. Based on our finding, facial and handwritten signature pictures are stored in JPEG2000 format and contain no meta-data.

### *2.2. ISO/IEC 14443 Standard*

Spanish ID cards rely on the ISO/IEC 14443 standard [22] to communicate through NFC. ISO/IEC 14443 is a four-part international standard for contactless smartcards operating at 13.56 MHz [22]. The NFC cards, also termed as Proximity Integrated Circuit Cards (PICC) or *tags*, are intended to operate up to 10 cm of a reader antenna, usually termed as Proximity Coupling Device (PCD).

ISO-14443-1 standard defines the size, physical characteristics, and environmental working card conditions. Part 2 of the standard defines the RF power and signalling schemes. In particular, two signalling schemes are defined (Type A and Type B). Both schemes are half duplex with a data

rate of 106 kbps (in each direction). DNIe3.0 follows the Type-B signalling scheme. ISO-14443-3 describes initialisation and anti-collision protocols, as well as commands, responses, data frame, and timing issues. Part 4 defines the high-level data transmission protocols. A PICC fulfilling all parts of ISO/IEC 14443 is named *IsoDep* card (for instance, contactless payment cards). Apart from specific protocol commands, the protocol defined in Part 4 is also capable of transferring Application Protocol Data Units (APDUs) as defined in ISO/IEC 7816-4 [23] and of application selection as defined in ISO/IEC 7816-5 [21]. In particular, DNIe3.0 uses $T = 0$ ISO/IEC 7816 and $T = CL$ ISO-14443 as transmission protocols.

## 3. Contactless Protocols used by DNIe3.0

This section briefly summarizes the protocols used by DNIe3.0 to communicate through the NFC interface. In particular, we first describe the Basic Access Control protocol and then the Password Authenticated Connection Establishment protocol. Both protocols are also used in electronic passports [7]. Furthermore, we also analyze here the entropy of their key space.

### *3.1. Basic Access Control Protocol*

Basic Access Control (BAC) protocol was included in Document 9303 [20], promoted by the International Civil Aviation Organization (ICAO), as a control mechanism to access to data stored in a secure chip through an RFID interface.

BAC was designed to protect less sensitive data and, in particular, to defend against skimming and eavesdropping threats [7]. To do so, it uses symmetric key device authentication. After a successful mutual authentication, the parties (reader and card) agree on a session key used to encrypt the subsequent exchange of information between these parties. The protocol uses as initial key some parts of the Machine Readable Zone (MRZ), located at the bottom of the reverse side of the DNIe3.0, which serves to verify physical access to the document. The necessary fields are, namely, the serial number of the identity card, date of birth, and expiry date (both expressed in American format, "aammdd").

The strength of the key used to encrypt and authenticate the contactless communication is directly proportional to the strength of the MRZ-derived password, due to the use of symmetric cryptography. Considering only the fields used in DNIe3.0, the maximum entropy of the MRZ can be estimated as follows:

- Serial number: this field is composed of 3 alphabetic characters plus 6 digits. Assuming random characters and digits, this corresponds to $log_2(26^3 + 10^6) = 34.0329$ bits.
- Date of birth: assuming a maximum age of 100, this corresponds to $\log_2(100 \cdot 365.25) = 15.1566$ bits. Open-source intelligence (OSINT) techniques may reduce this value up to zero.
- Expiry date: the DNIe3.0 can have different expiry dates, depending on the age of the individual. Namely, the expiry date is 5 years from the issue date when the age is lower than 30 years, or 10 years otherwise. There is no expiry date when the age of the individual is greater than 70 years. Assuming validity period of 10 years, this corresponds to $\log_2(10 \cdot 365.25) = 11.8347$ bits. We use this ballpark estimate as our working hypothesis, but the model can be refined (for instance, considering only working days).

Hence, at best, the strength of the key used by BAC is about 61 bits, which is less than the 80

bits recommended by both NIST and ECRYPT to protect against eavesdropping and other offline attacks [6, 14].

### 3.2. Password Authenticated Connection Establishment Protocol

The Password Authenticated Connection Establishment (PACE) protocol was proposed as an alternative to BAC, offering excellent protection against offline attacks [11]. The PACE protocol uses a weak password (with low entropy), verifies it, and generates cryptographically strong session keys.

In particular, the PACE protocol works as follows. First, the chip randomly chooses a number, encrypts it with a password-derived key and sends it to the terminal. Second, both the chip and the terminal map the random number to a specific set of parameters for asymmetric cryptography. Third, the chip and the terminal perform a Diffie-Hellman protocol based on those parameters. Later, the chip and terminal derive session keys, which are confirmed by exchanging and checking the authentication tokens.

As a password-derived key, it uses a 6-digit length number termed as Card Access Number (CAN), which is printed on the front side of the DNIe3.0. The entropy of this key is almost 20 bits ($\log_2 10^6 = 19.9316$), in contrast to the random numbers used by PACE with an entropy of 128 bits.

## 4. Security Assessment

This section introduces our security assessment of the Spanish contactless ID card. Note that the chip within DNIe3.0 will answer to requests with both the BAC and the PACE protocols. Since the key entropy used by PACE protocol is much lower than the key entropy used by BAC protocol, we focus on PACE protocol instead of BAC. Thus, we first study how DNIe3.0 behaves against a brute-force attack on the password-derived key used by the PACE protocol.

Recall that to establish a PACE protocol connection, the chip generates a nonce of 128 bits and sends it encrypted with the CAN to the reader. Therefore, security of the system also depends on the properties of the pseudo-random number generator used. Hence, we also evaluate the degree of randomness within a set of collected random numbers.

### 4.1. Brute Forcing Password-derived Keys

We developed an Android app[1] taking `AndroSmex`[2] as a code skeleton to perform the brute force attack. `AndroSmex` provides a basic implementation of connection through PACE protocol with the German ID card. As a hardware platform, we used a SONY Xperia Z3 Tablet Compact, which has a 2.5GHz Qualcomm Snapdragon 801 MSM8974AC quad-core processor, 3GB RAM memory, and a Broadcomm NFC chip.

We first measured how long it took to perfom 500 PACE protocol connection attempts. Figure 2 plots the time spent in each attempt. Our findings show that every PACE protocol connection took, on average, $1.4509$ seconds, independently of the password-derived key used. This time was (roughly) divided as follows: $200$ ms to generate and operate with random numbers, $1200$ ms to perform Diffie-Hellman protocol, and $100$ ms to generate, exchange, and check the authentication tokens.

These timing results show that even when the password-derived key used is incorrect, the imple-

[1] Source code is released under GPLv3 license and available at `https://github.com/VictorSanchez94/DNIe3.0_brute_force_v2`.
[2] Source code available at `https://github.com/tsenger/androsmex`.

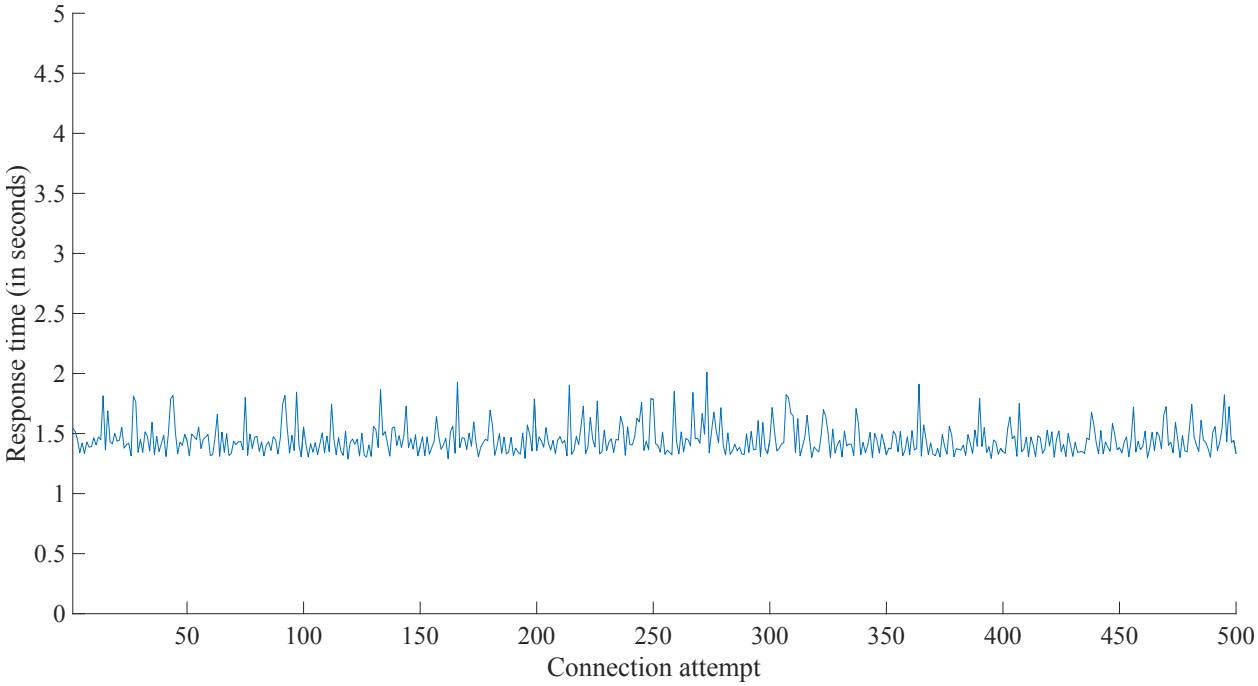



***Fig. 2.*** *Time spent in each PACE protocol connection attempt.*

mentation of PACE protocol continues execution until the last step, in which authentication tokens mismatch and then connection is closed. Thus, the current implementation of PACE protocol in DNIe3.0 does not exfiltrate whether the password-derived key used is correct until the protocol ends. This is technically correct and desired, since no clue is given to a brute-force attacker.

However, these results also evidence that there exists no defence implemented against on-line brute-force attacks. Regardless of connection attempts, the execution time of the PACE protocol remains the same. Hence, supposing a compromised Android smartphone with NFC capabilities and assuming a DNIe3.0 continuously in NFC range, in the worst case personal data could be stolen in near to 17 days.

This scenario is unlikely, since of course to communicate with a NFC card during 17 days without any interruption (and without any notice from the owner) is almost impossible. Nonetheless, targeted attacks may occur to specific individuals of interest. Furthermore, these attacks might be more feasible if DNIe3.0 fingerprinting is available and the attacker can stop and resume the brute-force attack whenever the card is at reach. We aim to further investigate this issue as future work.

**Suggested improvement:** We suggest to improve the PACE protocol algorithm to defend against on-line brute-force attacks. Thus, we envision that the revised PACE protocol may take different times to complete, depending on sequential connection attempts. French and Belgian electronic passports, for instance, already use this defense mechanism [5]. Consider that the execution time (in seconds) of the revised PACE protocol is given by a function $f$ as follows:

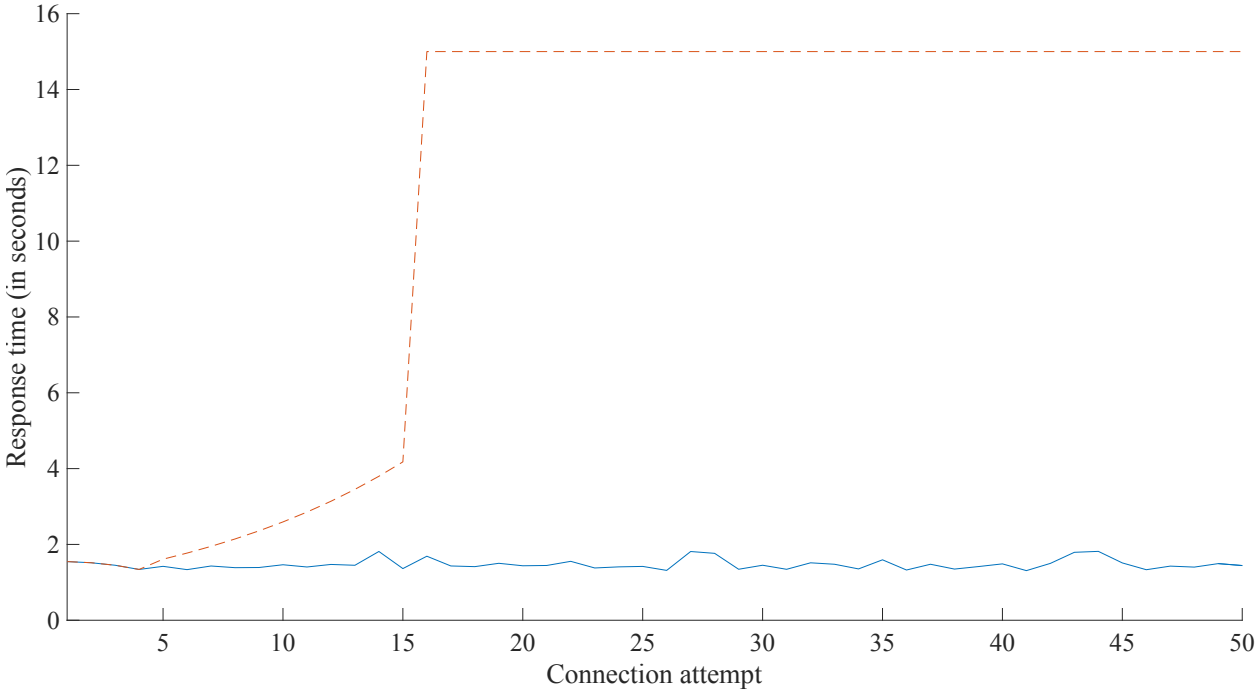



***Fig. 3.*** *Time spent in each PACE protocol connection attempt with a defense against brute-force attacks (excerpt of first 50 attempts).*

$$f(i) = \begin{cases} t & \text{when } i \leq 5, \\ \max(t, 1.1^i) & \text{when } i \leq 15, \\ 15 & \text{when } i > 15 \end{cases}$$

where $i$ is the sequential number of the connection attempt and $t$ is the execution time of PACE protocol. Note that we have arbitrarily set the connection attempt limits to 5 and 15. The specific limits are an implementation decision.

Figure 3 plots both the execution time of PACE protocol as giving by $f$ (solid line) and the execution time achieved by previous experimentation (dashed line) for an excerpt of 50 connection attempts. As observed, this little improvement would make infeasible an on-line brute-force attack against the DNIe3.0.

We communicated our findings to the National Coinage and Stamp Factory – Royal Mint, the Spanish National agency in charge of the development of the electronic Spanish ID card. They acknowledged our suggestions and told us to be taken into consideration for future DNIe3.0 implementation revisions.

### *4.2. Randomness analysis of the nonces used by PACE*

The PACE authentication protocol includes single-use bit sequences, or *nonces*, in order to make each communication step unique. Nonces help, among other things, to prevent replay and offline attacks. Predictable random sequences can significantly weaken authentication protocols as evinced by the attacks to the WEP wireless security protocol that predict its initialization vector and compromise the security of a Wi-Fi connection [9, 10].

In this section, we analyze the random nonces generated by the DNIe3.0 during the PACE protocol. As previously described in Section 2.1, the DNIe3.0 includes Infineon's SLE78CLFX408AP chip [13], which is used in a similar context in the German electronic passport, where its use of the PACE protocol was certified to be in accordance with the Common Methodology for IT Security evaluation [3, 4].

In this part of the study, we are concerned with the pseudo-random number generator in the card, which satisfies the requirements to be considered as a class PTG.2 chip according to the BSI (*Bundesamt für Sicherheit in der Informationstechnik*) recommendation AIS 31 for physical random number generators [17]. This means the chip should include a physical source of entropy that is later fed into a software random number generator. The output is then processed and checked for errors and statistical deviations from randomness.

While a good certification procedure is essential, there have been examples of certified electronic ID cards with weak random number generators. For instance, the Taiwan ID card had a good random number generation procedure, but some cards did not enforce it and, as a result, there was a series of cards with weak keys [8]. For that reason, it is worth making additional evaluations to discover problems early on.

In order to give an independent test of the random number generator used by the card during the PACE protocol, we collected the nonces from a series of failed PACE connection attempts. For each connection request, the card answers with a new challenge that includes a random number. Using the known CAN number from the card, we were able to decode these random nonces and abort the connection by sending a malformed message. In total, we collected $10^5$ nonces of 16 bytes each.

We analyzed these nonces to assess their randomness and found them to be of robust against the most common tests. In the following, we briefly describe these tests.

As preliminary test, we checked there was no repeated nonce in the $10^5$ captured values as expected. Each nonce has 16 bytes and a loose birthday paradox estimation gives us an expected probability of collision of the order of $10^{-3}$ for our long capture time.

Checking the resulting sequences for randomness is more tricky. There is no way to determine whether a finite sequence has been produced randomly or not. The bits 00 are no more or less random than 10. There are, however, multiple statistical tests that can estimate how likely it is that our bit sequence comes from a uniform random process [27].

From the possible testing options, we chose a few methods compatible with our (relatively short) collection of random bits. First, we used the utility `ent` [41] on the binary nonces with a result:

```
$ ent nonces.bin
Entropy = 7.999894 bits per byte.

Optimum compression would reduce the size
of this 1600000 byte file by 0 percent.

Chi square distribution for 1600000 samples is 234.59, and randomly
would exceed this value 75.00 percent of the times.
...
```

The entropy per byte is almost 8 and there is no appreciable size reduction with compression, which is consistent with a random output. A more sensitive test is Pearson's $\chi^2$ test, which checks for deviations from the expected statistics of a uniform distribution [16]. These results are as well within the expected values for a random sequence.

We also submitted the collected nonces to the FIPS 140-2 randomness tests [33] as implemented in the utility `rngtest` from `rng-tools` [1]. The program tested blocks of 20000 bits and all the

tests were passed (see below).

```
$  cat nonces.bin | rngtest
rngtest 4
Copyright (c) 2004 by Henrique de Moraes Holschuh
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

rngtest: starting FIPS tests...
rngtest: entropy source drained
rngtest: bits received from input: 12800000
rngtest: FIPS 140-2 successes: 639
rngtest: FIPS 140-2 failures: 0

...

rngtest: Program run time: 240792 microseconds
```

The FIPS tests check for the expected probability of sequences of consecutive zeros and ones of different lengths (runs) and the frequency of fixed-size bit combinations, among others, and are designed to detect failures of a device while in operation. Our collected nonces pass the tests with success.

We also tried a more visual test, the delayed-coordinates method [44], previously used to test the random nonces in the PACE protocol as implemented in the German ID card [32], which indeed shares many details with the Spanish ID card. In the delayed coordinates method, we take each nonce together with its three predecessors and map them into a three-dimensional phase space to look for attractors in the dynamics of the random number generator. Let $n(i)$ be the $i$th nonce. Hence, we convert it to a 128 bit positive integer and define three coordinates as:

$$x(i) = n(i) - n(i-1), \quad (1)$$
$$y(i) = n(i-1) - n(i-2), \quad (2)$$
$$z(i) = n(i-2) - n(i-3). \quad (3)$$

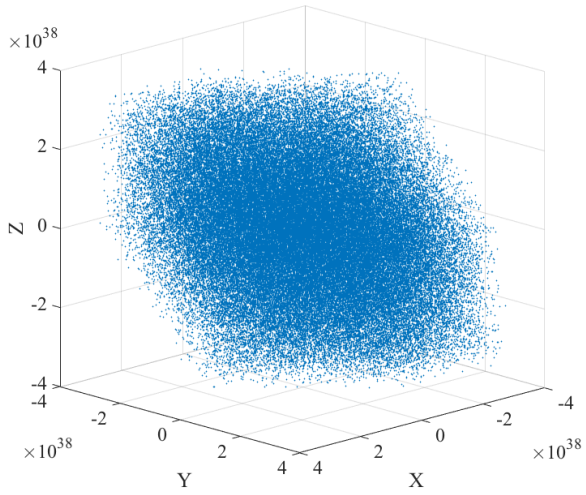
These coordinates define a series of points in the phase space. When the nonces that are generated around the same time are correlated, we expect the points in the phase space to cluster in some attractor.

Figure 4 shows the result of our experiment. The point distribution in the phase space is consistent with a uniform random number generator. While this test will not necessarily show long term correlations, when we consider it together with the previous results, it increases our confidence that the nonces in the protocol are indeed random.

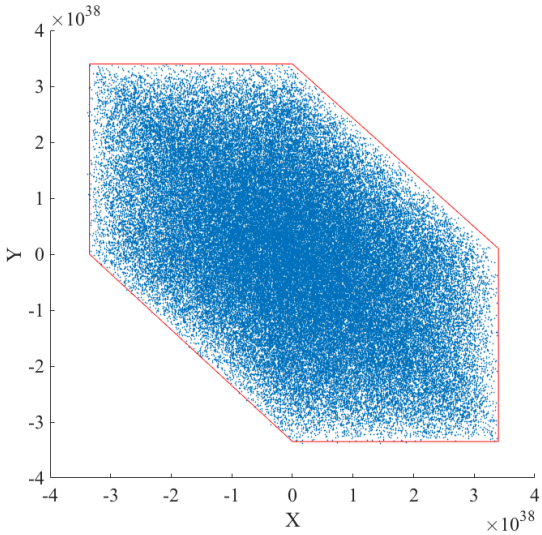
Finally, we tested the nonces with the NIST Statistical Test Suite [37], also with good results. The limited size of our data has prevented us to perform certain additional tests. For instance, in the NIST suite, we could not get a significant result for Maurer's universal test [30].

To conclude, while no finite amount of testing can discard hidden correlations, nonce generation in the chip seems to be free from obvious defects.

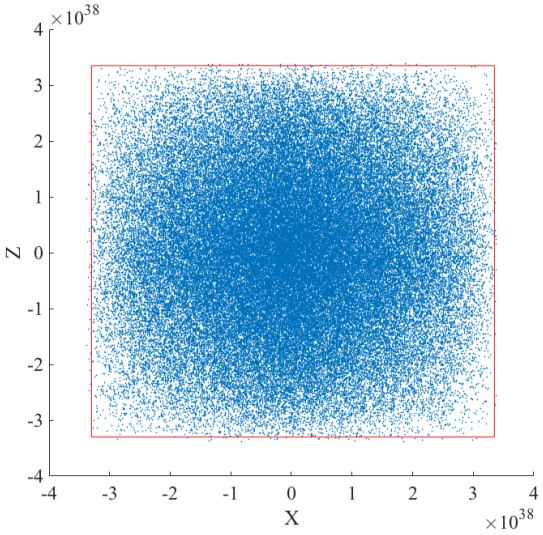
As final experiment, we also tested the behaviour of the DNIe3.0 just after power-up. The NFC chip gets its power from the signal of the reading device and the card must initialize its entropy pool every time it becomes active. With this test we want to check problems during the initialization phase. On certain occasions, random number generators can reset to a default state or start before gathering enough entropy and produce predictable outputs. For instance, a faulty initialization in



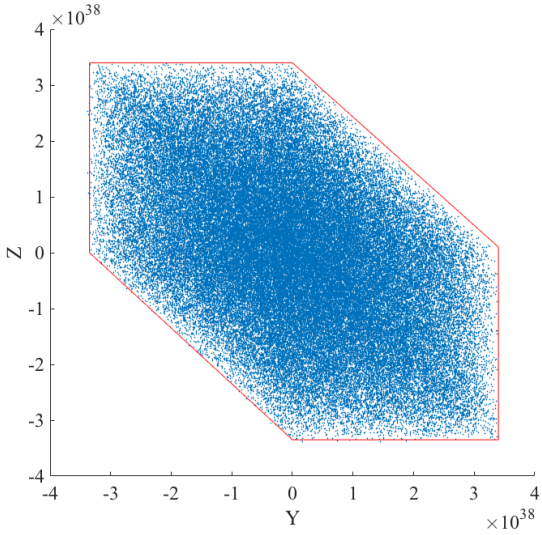

(a) *Delayed coordinates* 3D




(b) *Delayed coordinates* X-Y axes




(a) *Delayed coordinates* X-Z axes




(b) *Delayed coordinates* Y-Z axes

***Fig. 4.*** *Delayed coordinates graph and projections to each bidimensional plane. Each coordinate is defined from the nonces following Eq. 1. The points cover the phase space as expected for a random distribution.*

the electronic keno machine at the Montreal casino made the numbers repeat on power-up and an observant gambler took advantage of the failure to make more than half a million dollars [36]. To avoid these problems, the security requirements for cryptographic modules in FIPS 140-2 include a power-up test [33].

To test the nonces on initialization, we repeated the collection procedure with a failed PACE request but, this time, we made just one request before turning the communication off and leaving the card without any power. The collection is slower and thus, we only captured a total of 450 nonces where we found no repeated values. The results from `ent` and the FIPS tests are still consistent with a random sequence. While there is a limited amount of data due to the large waiting time, the initialization procedure looks adequate.

## 5. Related Work

Most previous existing works on the topic of NFC documents focus on electronic passports (e-passports). In [38], general NFC security threats as skimming or eavesdropping were remarked. Security and privacy issues of the European e-passport threats were largely detailed in [19]. Similarly, the risks of adding RFID to the US e-passports were reported in [31].

A good review on security features among e-passports of different countries was given in [26]. A FPGA implementation to crack BAC keys (mainly for German and Netherlands e-passports) was introduced in [28]. This implementation, termed as *COPACOBANA*, achieved a key search speed of 228 BAC keys per second. In [35], the authors proved that it was possible to fingerprint e-passports from different countries. As stated by the authors, fingerprinting e-passports opens the window to the possibility of *passport bomb*, designed to implode when some with a e-passport of a certain nationality comes close enough.

Regarding security assessment of e-passports, it is worth mentioning [39], where the authors identified security weaknesses in the Australian e-passport implementation using model-checking techniques. The low entropy problem in the password-derived key used by BAC was already pointed out in [7], where the authors also introduced the PACE protocol as a way to overcome the BAC protocol weaknesses.

To the best of our knowledge, we were the first to assess the security of the Spanish contactless identity card outside the official certification process. Other works, such as [32], evaluate the security of the German electronic contactless identity card.

## 6. Conclusions

In this paper, we evaluated the security of the PACE protocol as implemented in the Spanish contactless ID card (DNIe3.0). The protocol uses an initial common key (the Card Access Number, CAN) to encrypt a single-use bit sequence (nonce) generated by the card, later used to derive a secret Diffie-Hellman key to communicate the parties. We tested the protocol against brute-force attacks for an attacker that tries to guess the CAN and evaluated the randomness of the nonces the card generates.

A brute force attack seems unlikely, since for the measured execution times and the entropy of the CAN, an attacker would need to be in close proximity to the card for around 17 days. However, we found out the current implementation has no defense mechanism to hamper repeated failed requests. We suggest a simple modification that introduces a delay after the first few communication attempts and would make any brute force attack even less likely. We commented this modification

to the organism responsible for the implementation of the DNIe3.0, which confirmed it would be considered in future versions.

We also checked the randomness of the nonces the card generated during the protocol. The times involved in the protocol make it difficult to collect large sequences for exhaustive randomness tests, but the relatively short samples we captured seem to be free from obvious correlations. The collected sequences were submitted to different randomness test, including an entropy assessment, the FIPS140-2 battery, and a delayed coordinates test. All these tests were successfully passed. Finally, we tested the behaviour of the card at power-up. The random number generator seems to produce robust sequences from the first moment and we have found no deviation from the behaviour of the card in continuous operation.

## 7. Acknowledgments

The research of Ricardo J. Rodríguez was supported in part by Spanish MINECO project CyCriSec (TIN2014-58457-R) and by University of Zaragoza and Centro Universitario de la Defensa under project number UZCUD2016-TEC-06. The research of Juan Carlos Garcia-Escartin was supported by Project TEC2015-69665-R (MINECO/FEDER, UE).

## 8. References

[1] rng-tools. `https://wiki.archlinux.org/index.php/Rng-tools`.

[2] *Spanish Penal Code (Organic Law No. 10/1995 of November 23, 1995)*, November 1995. Available at `http://www.wipo.int/wipolex/en/details.jsp?id=15759`.

[3] Atos IT Solutions and Services GmbH. Certification report BSI-DSZ-CC-0967-2016 for CardOS DI V5.3 EAC/PACE Version 1.0 of the BSI, 2016. `https://www.commoncriteriaportal.org/files/epfiles/0967a_pdf.pdf`.

[4] Atos IT Solutions and Services GmbH. Security Target 'CardOS DI V5.3 EAC/PACE Version 1.0', Rev. 2.01, Edition 04/2016, 2016. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte09/0967b_pdf.pdf;jsessionid=8F38A3EA5734CA889E8EA7AB5E6B6190.1_cid341?__blob=publicationFile&v=2`.

[5] Gildas Avoine, Antonin Beaujeant, Julio Hernandez-Castro, Louis Demay, and Philippe Teuwen. A Survey of Security and Privacy Issues in ePassport Protocols. *ACM Comput. Surv.*, 48(3):47:1–47:37, February 2016.

[6] Elaine Barker. Recommendation for Key Management. Technical Report Special Publication 800-57 Revision 4, National Institute of Standards and Technology, January 2016. Available at `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf`.

[7] Jens Bender and Dennis Kügler. Introducing the PACE solution. *Keesing Journal of Documents & Identity*, 30:26–29, 2009.

[8] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren. *Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild*, pages 341–360. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[9] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, MobiCom '01, pages 180–189, New York, NY, USA, 2001. ACM.

[10] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker. Security Flaws in 802.11 Data Link Protocols. *Commun. ACM*, 46(5):35–39, May 2003.

[11] Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi. E-Passport: The Global Traceability Or How to Feel Like a UPS Package. In Jae Kwang Lee, Okyeon Yi, and Moti Yung, editors, *Proceedings of the 7th International Workshop on Information Security Applications (WISA 2006). Revised Selected Papers*, pages 391–404, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[12] Cuerpo Nacional de Policía (Spanish National Police Corps). DNIe Basic Reference Guide, June 2015. In Spanish. Available at `https://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_5.pdf`.

[13] Cuerpo Nacional de Policía (Spanish National Police Corps). NFC DNIe User Guide, February 2015. In Spanish. Available at `https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf`.

[14] ECRYPT. Yearly report on algorithms and keysizes. Technical report, European Network of Excellence in Cryptology, 2012. Available at `http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf`.

[15] Alberto Freire. El delito de robo de identidad (The crime of identity theft). Online, October 2015. In Spanish. Available at `http://www.infoderechopenal.es/2015/10/delito-robo-identidad.html`.

[16] Karl Pearson F.R.S. X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine Series 5*, 50(302):157–175, 1900.

[17] Bundesamt für Sicherheit in der Informationstechnik (BSI). Functionality classes and evaluation methodology for physical random number generators, AIS 31, V3, 2013. Documents available at `https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/AnwendungshinweiseundInterpretationen/AIS/AIS.html`.

[18] Ernst Haselsteiner and Klemens Breitfuß. Security in Near Field Communication (NFC) – Strengths and Weaknesses. In *Proceedings of the Workshop on RFID Security and Privacy (RFIDSec)*, 2006.

[19] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama, and Shinichi Kawamura, editors, *Proceedings of the First International Workshop on Security (IWSEC)*, pages 152–167, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[20] International Civil Aviation Organization. *ICAO Doc 9303 Machine Readable Travel Documents - Part 1: Machine Readable Passports - Volume 2: Specifications for electronically enabled passports with biometric identification capabilities*, 6th edition, 2006.

[21] International Organization for Standardization. ISO/IEC 7816-5-2013: Identification cards – Integrated circuit cards – Part 5: Registration of application providers, 2004.

[22] International Organization for Standardization. ISO/IEC 14443-3: Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision, April 2011.

[23] International Organization for Standardization. ISO/IEC 7816-4-2013: Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, 2013.

[24] M. Jakobsson and S. Myers. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley, 2006.

[25] Japanese Industrial Standard. JIS X 6319-4:2010: Specification of implementation for integrated circuit(s) cards – Part 4: High speed proximity cards. [Online; accessed at January 26, 2015], October 2010. `http://www.webstore.jsa.or.jp/webstore/PrevPdfServlet?dc=JIS&fn=pre_jis_x_06319_004_000_2010_e_ed10_i4.pdf`.

[26] A. B. Jeng and Lo-Yi Chen. How to enhance the security of e-Passport. In *2009 International Conference on Machine Learning and Cybernetics*, volume 5, pages 2922–2926, July 2009.

[27] Donald E Knuth. *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[28] Yifei Liu, Timo Kasper, Kerstin Lemke-Rust, and Christof Paar. E-Passport: Cracking Basic Access Control Keys. In Robert Meersman and Zahir Tari, editors, *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS: OTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS 2007, Vilamoura, Portugal, November 25-30, 2007, Proceedings, Part II*, pages 1531–1547, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[29] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger. NFC Devices: Security and Privacy. In *Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES)*, pages 642–647, March 2008.

[30] U. Maurer. A Universal Statistical Test for Random Bit Generators. *Journal of Cryptology*, 5(2):89–105, 1992.

[31] M. Meingast, J. King, and D. K. Mulligan. Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport. In *Proceedings of the 2007 IEEE International Conference on RFID*, pages 7–14, March 2007.

[32] Frederik Möllers. An Analysis of Traceability of Electronic Identification Documents. Master's thesis, Faculty of Electrical Engineering, Computer Science and Mathematics, Paderborn University, 2012.

[33] National Institue of Standards and Technology. FIPS PUB 140-2. Security Requirements for Cryptographic Modules, 2001. Available at `http://csrc.nist.gov/groups/STM/cmvp/standards.html`.

[34] NFC World. NFC phones: The definitive list. [Online; accessed at January 25, 2017], January 2017. http://www.nfcworld.com/nfc-phones-list/.

[35] Henning Richter, Wojciech Mostowski, and Erik Poll. Fingerprinting Passports. In *NLUUG Spring Conference on Security*, 2008.

[36] Christiane Rousseau and Yvan Saint-Aubin. *Random Number Generators*, pages 1–23. Springer New York, New York, NY, 2008.

[37] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010. Available at http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.

[38] Serge Vaudenay. E-Passport Threats. *IEEE Security & Privacy*, 5(6):61–64, 2007.

[39] P. Vijayakrishnan, Josef Pieprzyk, and Huaxiong Wang. Formal Security Analysis of Australian e-Passport Implementation. In *Proceedings of the Sixth Australasian Conference on Information Security - Volume 81*, AISC '08, pages 75–82, Darlinghurst, Australia, Australia, 2008. Australian Computer Society, Inc.

[40] José Vila and Ricardo J. Rodríguez. Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited. In *Proceedings of the 11th International Workshop on RFID Security (RFIDsec)*, volume 9440 of *Lecture Notes in Computer Science*, pages 87–103. Springer, 2015.

[41] John Walker. ENT. A Pseudorandom Number Sequence Test Program, 2008. http://www.fourmilab.ch/random/.

[42] WenJie Wang, Yufei Yuan, and N. Archer. A contextual framework for combating identity theft. *IEEE Security & Privacy*, 4(2):30–38, March 2006.

[43] Mark Wieting. Cuidado con perder el DNI. Online, April 2012. In Spanish. Available at http://www.abc.es/20120420/espana/abci-suplantacion-identidades-201204191917.html.

[44] Michal Zalewski. Strange Attractors and TCP/IP Sequence Number Analysis. http://lcamtuf.coredump.cx/oldtcp/tcpseq.