IET Journals
The Institution of Engineering and Technology

Security Assessment of the Spanish Contactless Identity Card

ISSN 1751-8644
doi: 0000000000
www.ietdl.org

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

[1] *Centro Universitario de la Defensa, Academia General Militar, Zaragoza, Spain*
[2] *Dpto. Teoría de la Señal y Comunicaciones e Ing. Telemática, Universidad de Valladolid, Spain*
* *E-mail: rjrodriguez@unizar.es*

Abstract: The theft of personal information to fake the identity of a person is a common threat normally performed by individual criminals, terrorists, or crime rings 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 criminals, who might take advantage of the RFID communication to virtually steal personal information. In this paper, we consider as case study the recently deployed contactless Spanish identity card assessing its security against identity theft. In particular, we evaluated the security of one of the contactless access protocol as implemented in the contactless Spanish identity card, and found that no defenses against on-line brute-force attacks were incorporated. We then suggest two countermeasures to protect against these attacks. Furthermore, we also analyzed the pseudo-random number generator within the card, which passed all the 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 [1]. 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 are, 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 [3]. In Spain, data written on the DNI are enough to hire different on-line products (such 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 [4].

Examples of felonies performed by criminals after the theft of Spanish ID cards are reported in [5]. 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 Neapolitan mafia-related drug dealer.

Recently, the DNI was updated to incorporate a Near Field Communication (NFC) chip, as electronic passports (e-passports, for short) do [6]. 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 [7] and the Sony FeLiCa [8] 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 [9–11]. 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 [12]. 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.

Let us remark that we are not providing here new vulnerabilities of or attacks to contactless protocols, as in [13–17]. This paper presents the results of an independent security assessment of the implementation of the NFC-enabled DNI as a case study. Our goal is to verify whether such implementation is performing as expected, in terms of security, since strongly sensitive data depend on it. While some functionalities of the new card have been certified, the protocols we test have not, to our knowledge, undergone a formal certification for the concrete hardware and software combination in the Spanish DNI3.0 card. Some other functionalities related to digital signatures have passed an EAL4+ (AVA_VAN.5) level Common Criteria security evaluation [18] and a previous implementation of the PACE protocol which uses the same chip the NFC DNI card has also passed an EAL4+ evaluation, but for the software in German electronic travel documents [19]. These certifications suggest random number generation and the access protocols are correctly implemented, but the NFC-enabled DNI as a whole has not been yet certified. In this case study we cover some of the untested parts and give an independent evaluation of the session establishment protocols in the NFC implementation of the DNI.

Related Work: Most previous existing works on the topic of NFC documents focus on electronic passports (e-passports). In [13], general NFC security threats as skimming or eavesdropping were remarked. Security and privacy issues of the European e-passport

threats were largely detailed in [14]. Similarly, the risks of adding RFID to the US e-passports were reported in [20].

A good review on security features among e-passports of different countries was given in [15]. An FPGA implementation to crack BAC keys (mainly for German and Netherlands e-passports) was introduced in [21]. This implementation, termed as *COPACOBANA*, achieved a key search speed of 228 BAC keys per second. In [17], 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 explode when someone with a e-passport of a certain nationality comes close enough.

Regarding security assessment of e-passports, it is worth mentioning [22], 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 [16], 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 ID card outside the official certification process. Other works, such as [23], evaluate the security of the German electronic contactless ID card, which shares many elements with the Spanish implementation.

Outline: 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 the NFC-enabled DNI (namely, the Basic Access Control and the Password Authenticated Connection Establishment protocols). Security assessment is detailed in Section 4. Finally, Section 5 concludes the paper.

2 Background

In this section, we first review the evolution of Spanish ID card. Then, we briefly introduce the ISO/IEC 14443 standard [7] 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 travelers (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 10000 inhabitants and then to frequent female travelers, 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 was a 32K STMicroelectronics ST19WL34. According to official documents [24], data within the chip were divided into three different zones: a *public zone*, which contained the intermediate CA certificate, Diffie-Hellman keys, and the X.509 certificate (read with no restrictions); a *private zone*, which contained the signature and authentication certificates of the citizen (only accessible through a PIN); and a *security zone*, which contained 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 called 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 [25]. This chip is prepared to support the access protocols we discuss. In particular, the implementation of the PACE protocol for German electronic travel documents CardOS DI V5.3 EAC/PACE Version 1.0 has successfully passed the Common Criteria EAL4 certification [19]. It also 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 [25], in this case data are 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). All those data are divided into four different data groups. We comment these data groups in detail in Section 3.3.

2.2 ISO/IEC 14443 Standard

Spanish ID cards rely on the ISO/IEC 14443 standard [7] to communicate through NFC. ISO/IEC 14443 is a four-part international standard for contactless smartcards operating at 13.56 MHz [7]. 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 signaling schemes. In particular, two signaling 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 signaling scheme. ISO-14443-3 describes initialization 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 [26] and of application selection as defined in ISO/IEC 7816-5 [27]. 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 [16]. Furthermore, we also analyze here the entropy of their key space. Lastly, we describe the personal data which are transmitted via the contactless interface.

3.1 Basic Access Control Protocol

The Basic Access Control (BAC) protocol is included in Document 9303 [28], 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 [16]. 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. The protocol uses as initial key some parts of the Machine Readable Zone (MRZ), located at the bottom of the reverse side

(a) (b)

Fig. 1: (a) Front side and (b) reverse side of the Spanish contactless ID card (extracted from [25]).

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 dates expressed in a "yymmdd" format).

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. The level of protection depends on the ignorance of the attacker about the information on the MRZ. Therefore, even though the password is derived in a deterministic way, we can compute an entropy value that estimates how many bits an attacker needs to guess in a brute-force attack. This value measures the uncertainty in the data the attacker possesses. 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 $\log_2(26^3 \cdot 10^6) = 34.0329$ bits.
- Date of birth: assuming a maximum age of 100, this corresponds to $\log_2(101 \cdot 365.25) = 15.171$ bits. Open-source intelligence (OSINT) techniques may reduce this value up to zero.
- Expiry date: the DNIe3.0 can have different expiry dates from the date of issue, depending on the age of the individual [29]. Namely, the expiry date is 2 years for children under 5, 5 years from the issue date when the age is greater than 5 and 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 a 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 [30, 31]. This estimate can be refined. For instance, the date of birth determines the range in the expiry date. When we consider both parameters together, we see their entropy is $\log_2(2 \cdot 5 \cdot 365.25^2 + 5 \cdot 25 \cdot 365.25^2 + 10 \cdot 40 \cdot 365.25^2 + 31 \cdot 365.25) = 26.089$, which is roughly 1 bit less than the broad average. We can also take into account that the issue day must be a working day, which limits the possible expiry dates. DNI issuing offices close on Sundays and many of them on Saturdays (or they offer only morning hours). If we factor all the local and national holidays, we get a rough correction factor of 0.75. These refinements reduce the search space to around 59 or 60 bits. Similarly, the new DNIe3.0 has only been active from 2015 and the number of possible issue dates is, at the time of writing, less than 1000 days, which gives a further reduction of about 1 to 2 bits of uncertainty.

This is a small reduction when compared to attacks based on open-source intelligence methods. The date of birth of a particular target can be gathered from public sources or could even be asked as a registration step in the same smartphone malware disguising as another application that later carries the attack. With a known birth date, the unknown bits reduce to a range from 35 bits (for ages over 70 when the expiry date is fixed) to 46 bits for the 10 year expiry range. Alternatively, the attacker can try an attack in a location close to the issuing office to target cards that have just been issued and eliminate the almost 12 bits of uncertainty in the expiry date. The safest line of defense against open-source intelligence is the random serial number, which can be enough to thwart a casual attacker. In the worst case scenario, phone malware could make the phone take a picture when it detects a nearby card and then read all the data needed to reproduce the key from the machine readable zone just a legitimate reader does. This would be equivalent to physical theft of the card. These advanced attacks are possible but challenging. Instead, we will consider basic brute-force attacks where no part of the initial key is known.

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 [32]. 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). As suggested by the PACE protocol specification [33], CAN may be static (printed in the card), semi-static (printed on a label on the card) or dynamic (randomly chosen during each operation and displayed using electronic ink, OLED or similar technologies). DNIe3.0 uses a static CAN number, i.e., printed on the front side of the card. As far as we are aware, this number is randomly generated by the manufacturing machine that produces the DNIe3.0 smartcard. We tried to contact the manufacturer and the people involved in the project to ask them about how CAN numbers are generated. However, we have received no positive answer. Under this *security-by-obscurity* principle, we assume that they are generated as secure as possible, i.e., CAN numbers are uniformly distributed random numbers in the interval $[0, 10^6)$. Hence, the entropy of this key is almost 20 bits ($\log_2 10^6 = 19.9316$) in contrast to the random numbers used after the exchange in the initial PACE protocol, which give session keys with an entropy of 128 bits.

3.3 Data Transmitted via the Contactless Interface

The chip of the DNIe3.0 stores data following a standard logical data structure, as defined in ISO/IEC 7816-4 [26]. In particular, ISO/IEC 7816 supports two different file categories (*dedicated files* and *elementary files*). From these, elementary files are used for storing data, while dedicated files are used for defining logical structural hierarchy (they may be seen as *subdirectories*). Elementary files are also called *data groups*. Data contained in such data groups are both individually and collectively signed by the Spanish government (as in e-passports, where data groups are signed by the issuing government).

There exists four different data groups which are accessible once the BAC or PAC protocol connection is successful:

Data Group 1.This file contains all data regarding the citizen that is visible in the front of the DNIe3.0: name and surnames (represented as a string), nationality (string), gender (string), support number (unequivocally identifies the location in which the DNIe3.0 was issued), issuer (string, it contains "España"), optional data (with null value), and document type (string, it contains "ID").

Data Group 2.This file contains the facial image of the identity card owner, which follows the JPEG 2000 image compression standard, as defined in ISO/IEC 15444. We have empirically verified that file image contains no meta-data, thus making harder to an attacker to figure out information regarding the machine used to issue DNIe3.0 cards.

Data Group 7.This file contains the handwritten signature image. As before, this image file follows the ISO/IEC 15444 standard and has no meta-data associated to it.

Data Group 11.This file contains more personal information about the card owner. Some of this information contains values, as the home address (string), the unique number that unequivocally identifies the citizen for the Spannish government (string), and the birth place (string, for instance, value "ZARAGOZA<ZARAGOZA"). There exists also other fields that currently contain no data. These fields are, in particular: title, telephone, occupation, custody info, ICAO name, other info, and summary. Although these fields may contain data before long, strong privacy concerns and user dissatisfaction are likely to occur since some data might be very sensitive.

According to official documentation [25], these data are stored in a security zone only accessible through special locations. However, we were able to access the data in the security zone with standard reading commands from our laboratory, contrary to it was stated in official documents.

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 both BAC and PACE protocol requests. Since the key entropy used by the PACE protocol is much lower than the key entropy used by the BAC protocol, we focus on the 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 random number of 128 bits and sends it encrypted with the CAN to the reader. Therefore, the 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.

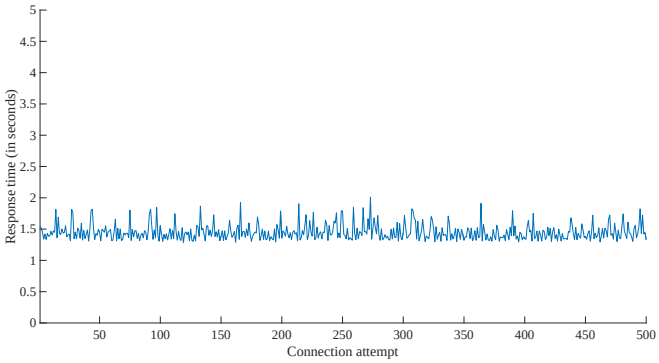


Fig. 2: Time spent in each PACE protocol connection attempt.

4.1 Brute Forcing Password-derived Keys

We developed an Android app* taking `AndroSmex`† as a code skeleton to perform the brute force attack. `AndroSmex` provides a basic implementation of connection through the PACE protocol with the German ID card. As our 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 perform 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, regardless 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 the 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 implementation of the PACE protocol continues execution until the last step, in which the authentication tokens do not match and the connection is closed. Thus, the PACE protocol as implemented in the 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 defense implemented against on-line brute-force attacks. Regardless of the number 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.

Once this attack is successful, different attacks are likely to occur. For instance, a malicious app could use the new credentials and, after authentication, try to sign certificates of the owner of the card. To do so, the card would ask for the PIN. After three consecutive incorrect PIN, the card would be blocked. Hence, the user shall go to special locations (where the DNIe3.0 was issued) to unblock it before being able to legitimately use it. This attack can be classified as a Denial-of-Service. Of course, in case that a malicious app could

*Source code is released under GPLv3 license and available at `https://github.com/ricardojrdez/DNIe3.0_brute_force_v2`.

†Source code available at `https://github.com/tsenger/androsmex`.

impersonate some legitimate app and could also know the PIN, other attacks are likely to occur, such as relay attacks: the attacker might use the authentication and sign certificates of the user remotely to perform an on-line identity theft.

Suggested improvements: We suggest two different countermeasures to defend against on-line brute-force attacks in PACE protocol. We first describe a countermeasure focused at software level and then another one focused at hardware level.

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 [6], in which a maximum number of consecutive attempts is defined and the response time depends on the connection attempt number. When the maximum is reached, the response time is set to a given value much greater than the normal operation time of the protocol. Hence, it makes infeasible an on-line brute-force attack when the maximum is reached.

Algorithm 1: Pseudo-code of our software proposal against on-line brute-force attacks.

```
   /* inside the function executed when the
      smartcard is powered */
1  ...
2  Initialize consecutive connections to zero
3  Initialize last connection to zero
4  ...

   /* called for each connection attempt */
5  Procedure attempt_PACE_connection(δ)
       Input: δ ∈ ℝ>0 defines the threshold used to detect
              consecutive connection attempts.
6      Store current timestamp in current timestamp variable (in
         milliseconds precision)
7      if (|last connection − current timestamp| ≤ δ) then
8          Reset NFC connection
9          Increment consecutive connections value
10         Sleep processor for consecutive connections seconds
11         Start NFC connection
12     end
13     Establish a new PACE connection
14     Set last connection value to current timestamp
15 end
```

The pseudo-code for our software proposal is shown in Algorithm 1. Lines 2, 3 are intended to be included in the procedure executed when the smartcard is powered on. They are devoted to initialize the values of the counter of consecutive connections and the timestamp of the last connection performed. Then, the procedure *attempt_PACE_connection* (lines 5–15) is added and executed for each connection attempt. This procedure receives a $\delta \in \mathbb{R}_{>0}$, used as threshold to detect (fast) consecutive attempts, in terms of milliseconds. The first line of the procedure gets the current time stamp, in milliseconds. Then, when the difference between last connection and current timestamps is lower than or equal to that δ, lines 8–11 take place: first, the NFC connection is reset; then, the consecutive connection counter is increased and the smartcard's processor is put to sleep for as many seconds as the value of the counter; last, the NFC connection is restarted. Finally, line 13 executes the PACE protocol and line 14 stores the current time under the name "last connection", which will be checked in the next connection attempt to keep track of previous requests.

Figure 3 plots both the execution time of PACE protocol as giving by Algorithm 1 (solid line) and as given by previous experimentation (dashed line) for an excerpt of 100 connection attempts. For the sake of simplicity, we only considered the execution time of line 10 of Algorithm 1. As observed, this little improvement would make infeasible an on-line brute-force attack against the DNIe3.0.

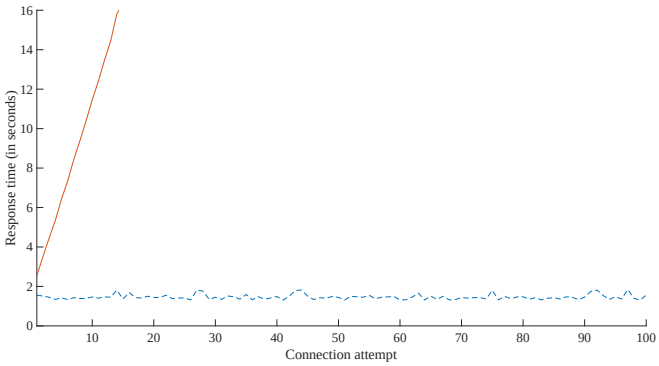


Fig. 3: Comparison between execution time with (solid line) and without defense (dashed line) against brute-force attacks.

The above software solution can be implemented almost immediately with little effort and minimal impact in the rest of the system. This notwithstanding, there are also simple design solutions that can be incorporated into newer cards to protect against brute-force attacks.

We suggest a second countermeasure where multiple connection attempts are hampered by controlling the power coupling between the reader and the card. In particular, the card will react to multiple connection attempts by reducing the signal available to the reader, thus forcing the attacker to come closer to the card. Imposing shorter distances makes automated attacks harder and makes also the attacker more conspicuous.

On the other hand, a legitimate reader trying to communicate with the card would have little additional troubles. If a rightful reader fails multiple connection attempts, the card is likely to be too far away for correct communication. Reducing the power would cut the connection and force the card owner to place it closer to the reader, the usual response when a contactless reader is not working. Reducing the signal is not a big problem in supervised communication, where the user must place the card in the reader. The need for user involvement is, in fact, one of the purposes of using near fields.

The suggested power reduction can be implemented with a small modification to the current hardware. The DNIe3.0 card, like many NFC cards and tokens, is passive, i.e. it does not have a power source of its own and communication with readers is done using *load modulation*. The coils in the card and the reader exchange information through inductive coupling. The reader can supply power to its coil, but the card cannot. As defined in the ISO/IEC 14443-2 standard [34], the reader sends data to the card by modulating the amplitude of the coupled RF field at the source, controlling the power supplied to the antenna. The communication from the card to the reader is done by altering the load connected to the card's antenna. The card can use a transistor to connect and disconnect a resistor to the antenna circuit. This load at the antenna modifies the radio-frequency coupling. The card can increase the load and absorb a larger part of the shared energy, which reduces the amplitude in the signals the reader measures. The fluctuations in the load are then used to encode data.

The basic load modulation circuit can be modified to prevent brute-force attacks. With minimal modifications, we can add a second load that can also be selectively added or not. If the card detects multiple connection attempts, it can connect the additional load (the *dampening load*). The available power in the field would decrease, but load modulation is still possible. Choosing right load values, the reduced power level when the dampening load is connected would further decrease when the modulation load is also part of the circuit. The result is a new load modulated signal at smaller amplitude levels.

The time and distance constraints of the proposed countermeasures make brute-force attacks more difficult without appreciable impact on the legitimate user. Both countermeasures can be combined for a greater effect and they do not restrict to the DNIe3.0 card, but can be extended to many other NFC and RFID secure protocols.

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 compromise the security of a Wi-Fi connection by predicting its initialization vector [35, 36].

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 [25], 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 at level EAL4+ [19, 37].

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 [38]. 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.

Although these certifications suggests the card can handle the PACE connection properly and produce good random numbers, as far as we know there has been no public formal evaluation of the chip/software combination as used in the NFC version of the DNI. Additionally, 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 [39]. 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 robust against the most common tests. In the following, we briefly describe these tests.

As a 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 [40].

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 χ^2 test, which checks for deviations from the expected statistics of a uniform distribution [42]. 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 [43] as implemented in the utility `rngtest` from `rng-tools` [44]. 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 [45], previously used to test the random nonces in the PACE protocol as implemented in the German ID card [23], 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 ith nonce. We can convert it to a 128 bit positive integer and define three coordinates as:

$$\begin{aligned} x(i) &= n(i) - n(i-1), \\ y(i) &= n(i-1) - n(i-2), \\ z(i) &= n(i-2) - n(i-3). \end{aligned} \tag{1}$$

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.

Figures 4 and 5 show the result of our experiment (the 3D graph and the projections to each bidimensional plane, respectively). 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 [46], 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 [47].

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 behavior of the DNIe3.0 just after power-up. The NFC chip gets its power from the signal

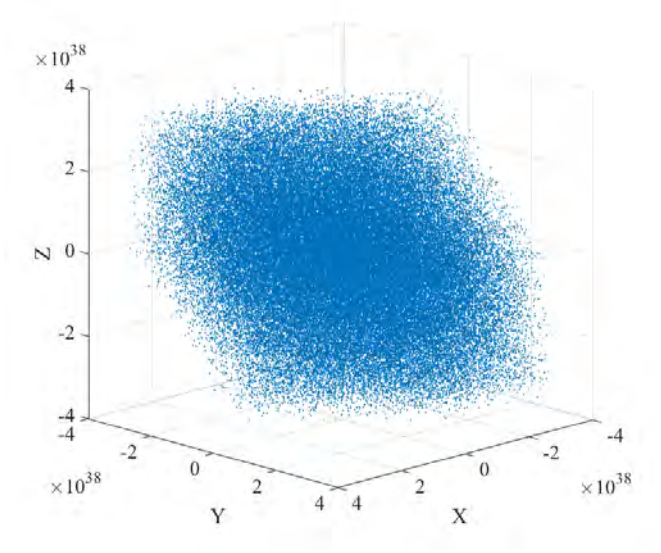


Fig. 4: Delayed coordinates graph. Each coordinate is defined from the nonces following Eq. (1). The points cover the phase space as expected for a random distribution.

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 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 [48]. To avoid these problems, the security requirements for cryptographic modules in FIPS 140-2 include a power-up test [43].

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 procedure is much 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 Conclusions

In this paper, we have evaluated the security of the PACE protocol as implemented in the Spanish contactless ID card (DNIe3.0) as a case study. 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 that is used in the communication between 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 two different countermeasures. First, we propose to introduce a software method that detects consecutive connection attempts and when detected, delays the connection with the smartcard. Second, we propose to reduce the signal power from the card to the reader when an attack is detected. Both modifications make any brute force attack even less likely and almost infeasible. These methods can be used alone or they can be combined with other previously published methods, such as introducing a delay after a few connection attempts[6]. We commented these improvements to the organism responsible for the implementation of the DNIe3.0, which confirmed that they would be considered in future versions.

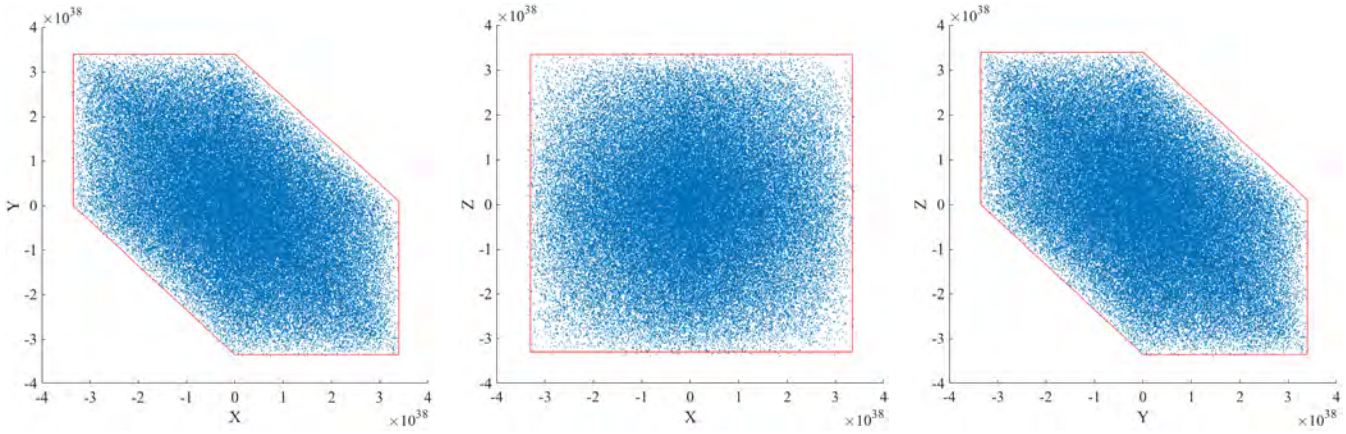
We have also checked the randomness of the nonces the card generated during the protocol. The times involved in the protocol make it difficult to collect large sequences for exhaustive randomness tests, but the relatively short samples we captured seem to be free from obvious correlations. The collected 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 behavior 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 behavior of the card in continuous operation.

Acknowledgments

The authors are grateful to the anonymous reviewers whose helpful comments have improved this manuscript. The authors are also grateful to staff from the Spanish Government National Cryptologic Center - Computer Security Incident Response Team for helping them to communicate their findings. 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) and by Junta de Castilla y León VA089U16.

6 References

1 Jakobsson, M., Myers, S.: 'Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft'. (Wiley, 2006)
2 'Spanish Penal Code (Organic Law No. 10/1995 of November 23, 1995)'. (, 1995. available at `http://www.wipo.int/wipolex/en/details.jsp?id=15759`.
3 Wang, W., Yuan, Y., Archer, N.: 'A contextual framework for combating identity theft', *IEEE Security & Privacy*, 2006, **4**, (2), pp. 30–38
4 Freire, A.. 'El delito de robo de identidad (The crime of identity theft)'. (, 2015. in Spanish. Available at `http://www.infoderechopenal.es/2015/10/delito-robo-identidad.html`. Online
5 Wieting, M.. 'Cuidado con perder el DNI'. (, 2012. in Spanish. Available at `http://www.abc.es/20120420/espana/abci-suplantacion-identidades-201204191917.html`. Online
6 Avoine, G., Beaujeant, A., Hernandez.Castro, J., Demay, L., Teuwen, P.: 'A Survey of Security and Privacy Issues in ePassport Protocols', *ACM Comput Surv*, 2016, **48**, (3), pp. 47:1–47:37
7 International Organization for Standardization. 'ISO/IEC 14443-3: Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision' [Norm]. (Geneva, Switzerland, 2011. Available from: `http://www.iso.org/iso/catalogue_detail.htm?csnumber=50942`
8 Japanese Industrial Standard. 'JIS X 6319-4:2010: Specification of implementation for integrated circuit(s) cards – Part 4: High speed proximity cards'. (, 2010. `http://www.webstore.jsa.or.jp/webstore/PrevPdfServlet?dc=JIS&fn=pre_jis_x_06319_004_000_2010_e_ed10_i4.pdf`. [Online; accessed at January 26, 2015]
9 Haselsteiner, E., Breitfuß, K. 'Security in Near Field Communication (NFC) – Strengths and Weaknesses'. In: Proceedings of the Workshop on RFID Security and Privacy (RFIDSec). (, 2006.
10 Madlmayr, G., Langer, J., Kantner, C., Scharinger, J. 'NFC Devices: Security and Privacy'. In: Proceedings of the 3rd International Conference on Availability, Reliability and Security (ARES). (, 2008. pp. 642–647
11 Vila, J., Rodríguez, R.J. 'Practical Experiences on NFC Relay Attacks with Android: Virtual Pickpocketing Revisited'. In: Proceedings of the 11th International Workshop on RFID Security (RFIDsec). vol. 9440 of *Lecture Notes in Computer Science*. (Springer, 2015. pp. 87–103
12 NFC World. 'NFC phones: The definitive list'. (, 2017. `http://www.nfcworld.com/nfc-phones-list/`. [Online; accessed at January 25, 2017]
13 Vaudenay, S.: 'E-Passport Threats', *IEEE Security & Privacy*, 2007, **5**, (6), pp. 61–64
14 Hoepman, J.H., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R.W. 'Crossing Borders: Security and Privacy Issues of the European e-Passport'. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S., editors. Proceedings of the First International Workshop on Security (IWSEC). (Berlin, Heidelberg: Springer Berlin Heidelberg, 2006. pp. 152–167
15 Jeng, A.B., Chen, L.Y. 'How to enhance the security of e-Passport'. In: 2009 International Conference on Machine Learning and Cybernetics. vol. 5. (, 2009. pp. 2922–2926



(a) X-Y plane (b) X-Z plane (c) Y-Z plane

Fig. 5: Delayed coordinates 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.

16 Bender, J., Kügler, D.: 'Introducing the PACE solution', *Keesing Journal of Documents & Identity*, 2009, **30**, pp. 26–29

17 Richter, H., Mostowski, W., Poll, E. 'Fingerprinting Passports'. In: NLUUG Spring Conference on Security. (, 2008.

18 Centro Criptológico Nacional (Spanish National Cryptologic Centre). 'Documento 2014-39-INF-1766 v2. Informe de Certificación del producto DNIe-DSCF (dispositivo seguro de creación de firma) versión 3.0.'. (, 2017. in Spanish. Available at https://www.commoncriteriaportal.org/files/epfiles/2014-39_inf-1766_v2.pdf.

19 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

20 Meingast, M., King, J., Mulligan, D.K. '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. (, 2007. pp. 7–14

21 Liu, Y., Kasper, T., Lemke.Rust, K., Paar, C. 'E-Passport: Cracking Basic Access Control Keys'. In: On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS: OTM Confederated International Conferences 2007, Vilamoura, Portugal, November 25-30, 2007, Proceedings, Part II. (Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. pp. 1531–1547

22 Vijayakrishnan, P., Pieprzyk, J., Wang, H. 'Formal Security Analysis of Australian e-Passport Implementation'. In: Proceedings of the Sixth Australasian Conference on Information Security - Volume 81. AISC '08. (Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2008. pp. 75–82

23 Möllers, F. 'An Analysis of Traceability of Electronic Identification Documents' [MSc. Thesis]. Faculty of Electrical Engineering, Computer Science and Mathematics, Paderborn University, 2012

24 Cuerpo Nacional de Policía (Spanish National Police Corps). 'DNIe Basic Reference Guide'. (, 2015. in Spanish. Available at https://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_5.pdf.

25 Cuerpo Nacional de Policía (Spanish National Police Corps). 'NFC DNIe User Guide'. (, 2015. in Spanish. Available at https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf.

26 International Organization for Standardization. 'ISO/IEC 7816-4-2013: Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange' [Norm]. (Geneva, Switzerland, 2013. Available from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=54550

27 International Organization for Standardization. 'ISO/IEC 7816-5-2013: Identification cards – Integrated circuit cards – Part 5: Registration of application providers' [Norm]. (Geneva, Switzerland, 2004. Available from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=34259

28 'ICAO Doc 9303, Machine Readable Travel Documents Part 11 — Security Mechanisms for MRTDs'. (, 2015. available at https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf.

29 Ministerio del Interior (Spanish Ministry of Home Affairs). 'Real decreto 869/2013'. (, 2013. in Spanish. Available at https://www.boe.es/boe/dias/2013/11/23/pdfs/BOE-A-2013-12320.pdf. Boletín Oficial del Estado, 23rd November 2013.

30 ECRYPT. 'Yearly report on algorithms and keysizes'. (European Network of Excellence in Cryptology, 2012. available at http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf.

31 Barker, E. 'Recommendation for Key Management'. (National Institute of Standards and Technology, 2016. Special Publication 800-57 Revision 4. available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

32 Carluccio, D., Lemke.Rust, K., Paar, C., Sadeghi, A.R. 'E-Passport: The Global Traceability Or How to Feel Like a UPS Package'. In: Lee, J.K., Yi, O., Yung, M., editors. Proceedings of the 7th International Workshop on Information Security Applications (WISA 2006). Revised Selected Papers. (Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. pp. 391–404

33 'Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 1 – eMRTDs with BAC/PACEv2 and EACv1'. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015. Technical Guideline TR-03110-1

34 International Organization for Standardization. 'ISO/IEC 14443-3: Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface' [Norm]. (Geneva, Switzerland, 2016. Available from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50942

35 Borisov, N., Goldberg, I., Wagner, D. 'Intercepting Mobile Communications: The Insecurity of 802.11'. In: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking. MobiCom '01. (New York, NY, USA: ACM, 2001. pp. 180–189

36 Cam.Winget, N., Housley, R., Wagner, D., Walker, J.: 'Security Flaws in 802.11 Data Link Protocols', *Commun ACM*, 2003, **46**, (5), pp. 35–39

37 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

38 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

39 Bernstein, D.J., Chang, Y.A., Cheng, C.M., Chou, L.P., Heninger, N., Lange, T., et al. In: Sako, K., Sarkar, P., editors. 'Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild'. (Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. pp. 341–360

40 Knuth, D.E.: 'The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms'. (Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1997)

41 Walker, J.. 'ENT. A Pseudorandom Number Sequence Test Program'. (, 2008. http://www.fourmilab.ch/random/

42 Pearson, K.: '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*, 1900, **50**, (302), pp. 157–175

43 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

44 'rng-tools'. (, . https://wiki.archlinux.org/index.php/Rng-tools

45 Zalewski, M.. 'Strange Attractors and TCP/IP Sequence Number Analysis'. (, . http://lcamtuf.coredump.cx/oldtcp/tcpseq

46 Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E.. '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

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

48 Rousseau, C., Saint.Aubin, Y. In: 'Random Number Generators'. (New York, NY: Springer New York, 2008. pp. 1–23