# DNIe3.0 Security: More Problems Than Solutions?

Víctor Sánchez-Ballabriga[†], **Ricardo J. Rodríguez**[‡]

@RicardoJRdez ※ rjrodriguez@unizar.es ※ www.ricardojrodriguez.es





[†]Universidad de Zaragoza

[‡]Centro Universitario de la Defensa,
Academia General Militar (AGM)

March 04, 2017

**RootedCON 2017**
Madrid

# $whoami


- BSc. in Informatics Engineering by University of Zaragoza (UZ)
- **Part of this work was his Final Degree Project**
  - Check technical report here
- Working at a cybersec company

- **Ph.D. on Comp. Sci.** (UZ, 2013)
- **Assistant Professor** at Centro Universitario de la Defensa, AGM
- Main research lines:
  - Security-driven engineering
  - Malware (anti-)analysis
  - RFID/NFC Security

#sinCiencia
no hay futuro

# Agenda

# Agenda

# Introduction

## Identity theft

- To impersonate other individual
- **Theft of personal information (as name, date of birth) to fake identity of another party**

# Introduction

## Identity theft

- To impersonate other individual
- **Theft of personal information (as name, date of birth) to fake identity of another party**

- Increasing problem in Spain. **117 cases reported in 2014**
  - Check `http://www.voluntaddigital.com/suplantacion-de-identidad-y-delitos-en-internet`
- **Felony under the Spanish Criminal Code**
  - **Article 401**: **On identity fraud**
    - *Whoever usurps the identity of another shall be punished with a sentence of imprisonment of six months to three years*
    - On practice, only applicable when marital status is usurped (AFAIK)
  - **Article 197**: **On discovery and revelation of secrets**
    - *2. The same penalties shall be imposed upon whoever, without being authorised, seizes, uses or amends, to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in computer, electronic or telematic files or media, or in any other kind of file or public or private record. The same penalties shall be imposed on whoever, without being authorised, accesses these by any means, and whoever alters or uses them to the detriment of the data subject or a third party*

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**
  - 4.5M of cases estimated in Spain. **Average fraud of 8000€ per case**

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**
  - 4.5M of cases estimated in Spain. **Average fraud of 8000€ per case**
  - Think a moment: **what is the minimum required data for hiring...**

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**
  - 4.5M of cases estimated in Spain. **Average fraud of 8000€ per case**
  - Think a moment: **what is the minimum required data for hiring...**
    - ... a new Internet service (or any other telco service)?

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**
  - 4.5M of cases estimated in Spain. **Average fraud of 8000€ per case**
  - Think a moment: **what is the minimum required data for hiring...**
    - ... a new Internet service (or any other telco service)?
    - ... a mortgage?

# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**
  - 4.5M of cases estimated in Spain. **Average fraud of 8000€ per case**
  - Think a moment: **what is the minimum required data for hiring...**
    - ... a new Internet service (or any other telco service)?
    - ... a mortgage?
    - ... a loan?

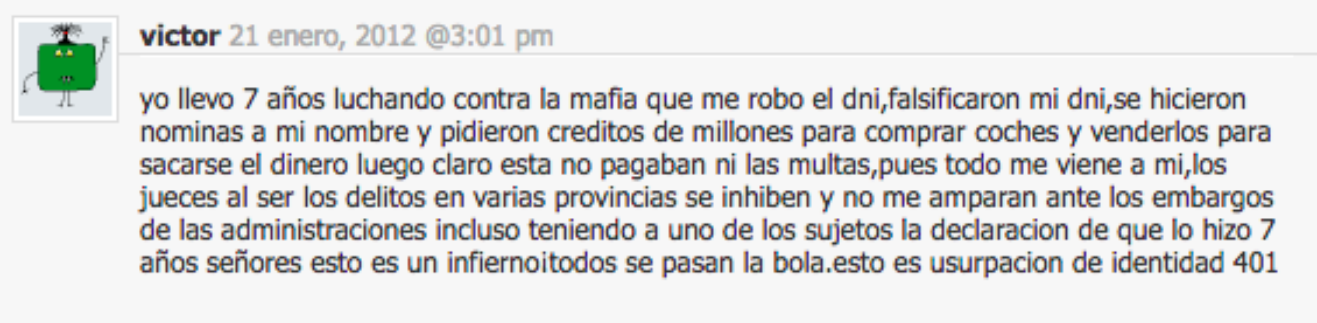
# Introduction

## Who?

- Criminals, terrorist, crime ring, ...

## Why?

- **Take advantage of impersonation to commit fraud or other felonies**
  - 4.5M of cases estimated in Spain. **Average fraud of 8000€ per case**
  - Think a moment: **what is the minimum required data for hiring...**
    - ... a new Internet service (or any other telco service)?
    - ... a mortgage?
    - ... a loan?
- **To generate false location traces**



**victor** 21 enero, 2012 @3:01 pm

yo llevo 7 años luchando contra la mafia que me robo el dni,falsificaron mi dni,se hicieron nominas a mi nombre y pidieron creditos de millones para comprar coches y venderlos para sacarse el dinero luego claro esta no pagaban ni las multas,pues todo me viene a mi,los jueces al ser los delitos en varias provincias se inhiben y no me amparan ante los embargos de las administraciones incluso teniendo a uno de los sujetos la declaracion de que lo hizo 7 años señores esto es un infiernoitodos se pasan la bola.esto es usurpacion de identidad 401

# Introduction

Real examples (credits: `http://www.abc.es/20120420/espana/abci-suplantacion-identidades-201204191917.html`)

- **Francesc F.G., from Barcelona**
  - Repetitively stole gym lockers
  - Used the stolen documentation to ask for taxpayer statement, work certificate, and census. Then, **he hired loans and credit cards on behalf of victims**
  - **Was charged with felonies of fraud, usurpation of marital status, and misappropriation of funds**
- **Álvaro G., Madrid** (39 years old)
  - **A copy of his identity taken in a hotel check-in was enough to open online banking, telephone, and gambling house accounts**

# Introduction

Real examples (credits: `http://www.abc.es/20120420/espana/abci-suplantacion-identidades-201204191917.html`)

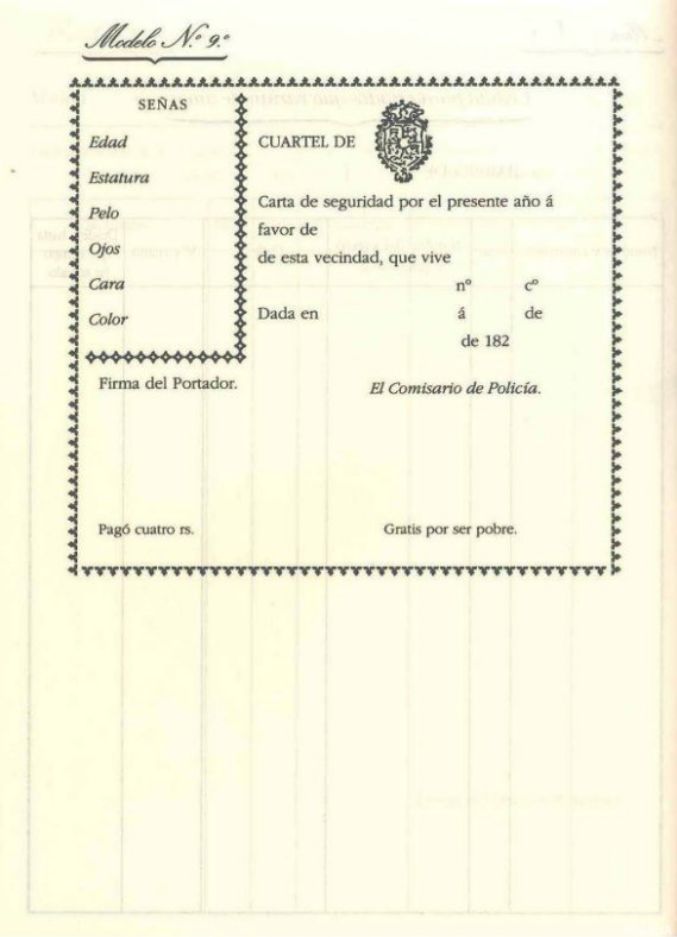
- **Noelia Carmena, Madrid**
  - Spanish ID card (DNI) stolen in the metro at 2006
  - **Was charged with organized crime ring regarding convenience marriages**
  - Hold under arrest for 24h and judged by identity theft, fraud, and documentary forgery. Accused of receiving 3500€ for a convenience marriage
- **Óscar Sánchez, somewhere in Cataluña**
  - **626 days in an Italian prison, was charged with drug dealing traffic**
  - **He sold his DNI**, which ended up being used by an Uruguayan folk linked with the Camorra for checking into hotels

# Agenda

# Evolution of the Spanish Identity Card (DNI)

## Book of Genesis

- **National Police Corps** (former *Policía General de Reino*): created in 1824 (Ferdinand VII of Spain)
  - **Allowed to issue official documents** with data as:
    - Age
    - Gender
    - Marital status
    - Occupation
    - Location


Modelo N.º 9.º

SEÑAS

*Edad*

*Estatura*

*Pelo*

*Ojos*

*Cara*

*Color*

CUARTEL DE

Carta de seguridad por el presente año á favor de de esta vecindad, que vive

Dada en nº á de de 182 cº

Firma del Portador.

*El Comisario de Policía.*

Pagó cuatro rs.

Gratis por ser pobre.

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Exodus

- *Cédulas personales* (1941)
  - **Issued by the local governments**
  - Optional photography
  - Different data (depends on the local government!)


Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


- *DNI version 0.0*
  - Decree of March 2, 1944
  - **Call for tender. 30000 ptas!**
    - **Requirements**: fit into wallet, enough space for fingerprint and picture. Unalterable inks
  - Awardee: *Aquilino Riusset Planchón*

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


- *DNI version 0.0*
  - Decree of March 2, 1944
  - **Call for tender. 30000 ptas!**
    - **Requirements**: fit into wallet, enough space for fingerprint and picture. Unalterable inks
  - Awardee: *Aquilino Riusset Planchón*
  - **1951. First DNI issued to "tío Paco"**

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


- *DNI version 0.0*
  - Decree of March 2, 1944
  - **Call for tender. 30000 ptas!**
    - **Requirements**: fit into wallet, enough space for fingerprint and picture. Unalterable inks
  - Awardee: *Aquilino Riusset Planchón*
  - **1951. First DNI issued to "tío Paco"**
    - No. 2 to Carmen Polo, no. 3 to Carmen Franco

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


## Assignment process

1. Prisoners and supervised release individuals

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


## Assignment process

1. Prisoners and supervised release individuals
2. Male individuals who frequently change home address (due to their profession or business)

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


## Assignment process

1. Prisoners and supervised release individuals
2. Male individuals who frequently change home address (due to their profession or business)
3. Male individuals in cities with 100000 or more inhabitants

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

Book of Leviticus: 1951–1961


## Assignment process

1. Prisoners and supervised release individuals
2. Male individuals who frequently change home address (due to their profession or business)
3. Male individuals in cities with 100000 or more inhabitants

- **Zaragoza: first city**
- **1961: from 10 to 99 are reserved for the Spanish Royal Family**
  - 10: King Juan Carlos I; 11: Queen Sofía. **13 avoided by superstition**

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Numbers

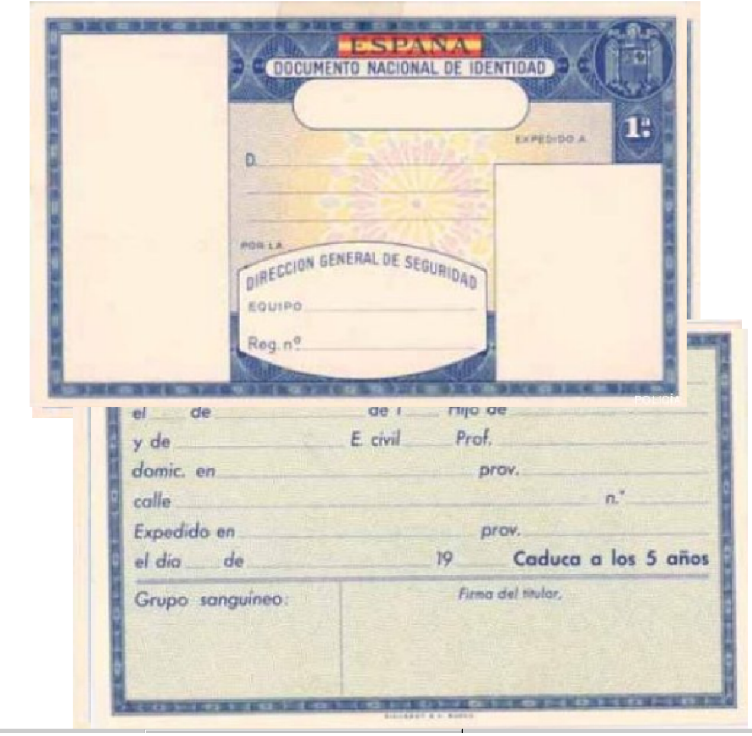

1962–1965

- Blue color
- Blood type and marital status added. Gender removed

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Numbers



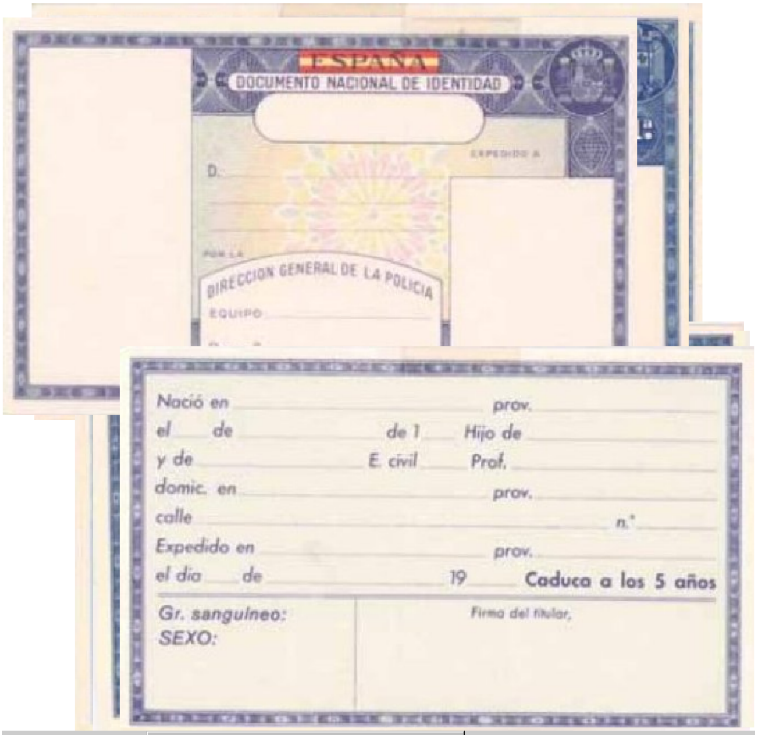

1962–1965
- Blue color
- Blood type and marital status added. Gender removed

1965–1980
- Administrative Head signature removed

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Numbers




| | |
|---|---|
| 1962–1965 | • Blue color<br>• Blood type and marital status added. Gender removed |
| 1965–1980 | • Administrative Head signature removed |
| 1981–1985 | • Constitutional coat of arms of Spain and gender added |

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Numbers


| | |
|---|---|
| 1962–1965 | • Blue color<br>• Blood type and marital status added. Gender removed |
| 1965–1980 | • Administrative Head signature removed |
| 1981–1985 | • Constitutional coat of arms of Spain and gender added |
| 1985–1991 | • Expiry date extended to 10 years ($\geq$ 30 years old)<br>• Occupation, marital status, and blood type removed<br>• Redundant tax letter added in 1990<br>• Numbers were first manually assigned. Computerized in 1991<br>  • Special department created to solve the “wrong numbers” issue |

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Deuteronomy


1991–1996

- **DNI version 1.0**
- Smaller. **No fingerprint**
- MRZ added (OCR very primal)

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Deuteronomy


| | |
|---|---|
| 1991–1996 | • **DNI version 1.0**<br>• Smaller. **No fingerprint**<br>• MRZ added (OCR very primal) |
| 1996–2000 | • **Color photograph**<br>• OCR characters extended |

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

## Book of Deuteronomy


| | |
|---|---|
| 1991–1996 | • **DNI version 1.0**<br>• Smaller. **No fingerprint**<br>• MRZ added (OCR very primal) |
| 1996–2000 | • **Color photograph**<br>• OCR characters extended |
| 2000-2006 | • Spanish identification label added (obverse)<br>• **Gender tags extended: M-F and V-M** |

Credits: `http://www.huffingtonpost.es/2015/01/12/evolucion-dni_n_6456474.html`

# Evolution of the Spanish Identity Card (DNI)

New Testament – First electronic DNI (version 2.0)

## 2006–2015

- **Physical security elements added to prevent card forging**
- **32K STMicroelectronics ST19WL34**
- Data divided in:
  - **Public zone**: intermediate CA certificate, Diffie-Hellman keys, X.509 certificate. **Read without restrictions**

# Evolution of the Spanish Identity Card (DNI)

New Testament – First electronic DNI (version 2.0)

## 2006–2015

- **Physical security elements added to prevent card forging**
- **32K STMicroelectronics ST19WL34**
- Data divided in:
  - **Public zone**: intermediate CA certificate, Diffie-Hellman keys, X.509 certificate. **Read without restrictions**
  - **Private zone**: signature and authentication citizen certificate. **Only accessible through a PIN**

# Evolution of the Spanish Identity Card (DNI)

New Testament – First electronic DNI (version 2.0)

## 2006–2015

- **Physical security elements added to prevent card forging**
- **32K STMicroelectronics ST19WL34**
- Data divided in:
  - **Public zone**: intermediate CA certificate, Diffie-Hellman keys, X.509 certificate. **Read without restrictions**
  - **Private zone**: signature and authentication citizen certificate. **Only accessible through a PIN**
  - **Security zone**: citizen data, facial photo, handwritten signature image. **Only accessible thr. special spots**

# Evolution of the Spanish Identity Card (DNI)

New Testament – First electronic DNI (version 2.0)

## 2006–2015

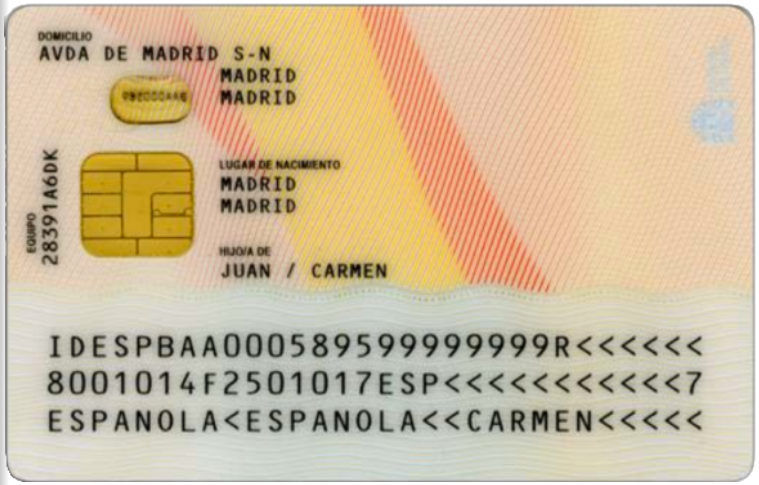
- **Physical security elements added to prevent card forging**
- **32K STMicroelectronics ST19WL34**
- Data divided in:
  - **Public zone**: intermediate CA certificate, Diffie-Hellman keys, X.509 certificate. **Read without restrictions**
  - **Private zone**: signature and authentication citizen certificate. **Only accessible through a PIN**
  - **Security zone**: citizen data, facial photo, handwritten signature image. **Only accessible thr. special spots**
- **Grey-scale facial photo**
- OCR-B characters

# Evolution of the Spanish Identity Card (DNI)

Book of Revelation (1) – DNI version 3.0

## 2015–????

- **New physical security elements**
- Electronic chip located at the reverse
  - **SLE78CLFx498AP** (400K, 8KB RAM)
  - **CC EAL5+ certification**
- Data divided in:
  - **Public zone**: intermediate CA certificate, Diffie-Hellman keys, X.509 certificate, and signature and authentication citizen certificate. **Read without restrictions**

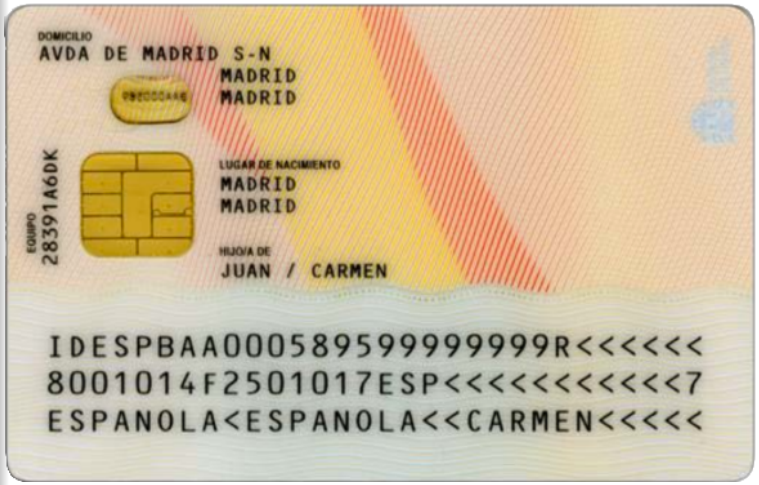



# Evolution of the Spanish Identity Card (DNI)

Book of Revelation (1) – DNI version 3.0

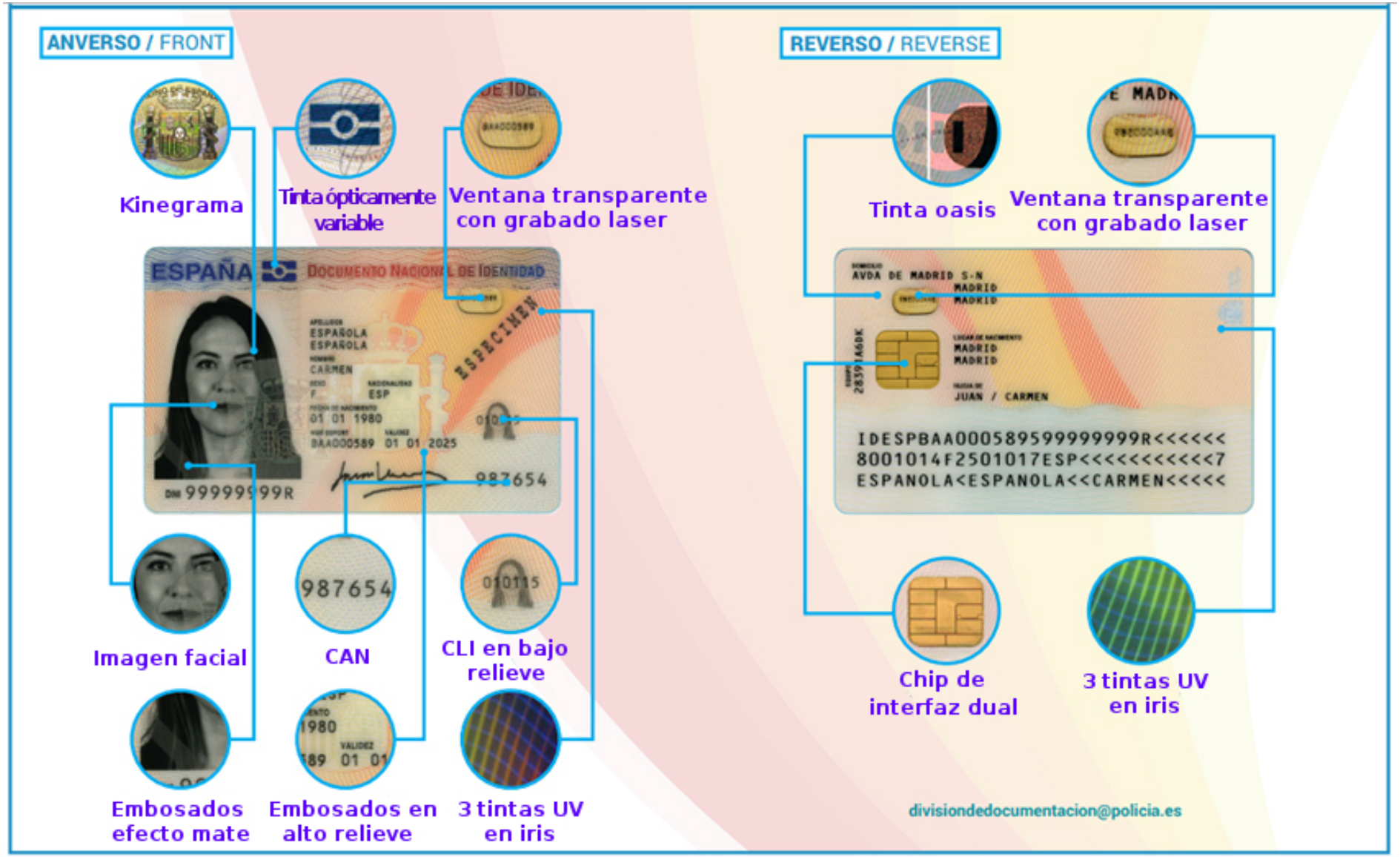
## 2015–????

- **New physical security elements**
- Electronic chip located at the reverse
  - **SLE78CLFx498AP** (400K, 8KB RAM)
  - **CC EAL5+ certification**
- Data divided in:
  - **Public zone**: intermediate CA certificate, Diffie-Hellman keys, X.509 certificate, and signature and authentication citizen certificate. **Read without restrictions**
  - **Security zone**: citizen data, facial photo, handwritten signature image. *"Only accessible through special spots"* [from official report] **(really?)**

# Evolution of the Spanish Identity Card (DNI)

## Book of Revelation (2) – DNI version 3.0



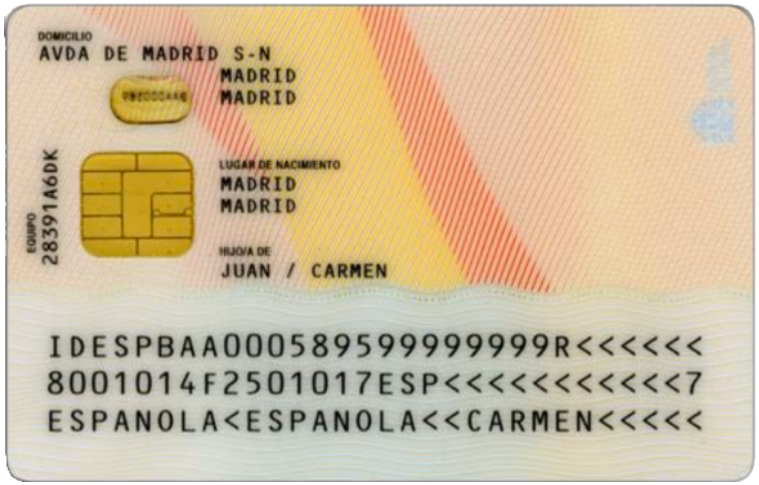
# Evolution of the Spanish Identity Card (DNI)

Book of Revelation (3)

## 2015–????

- **New number added in the front** (right-bottom corner)
- First DNIe3.0: Mireia Belmonte

**NFC capabilities**

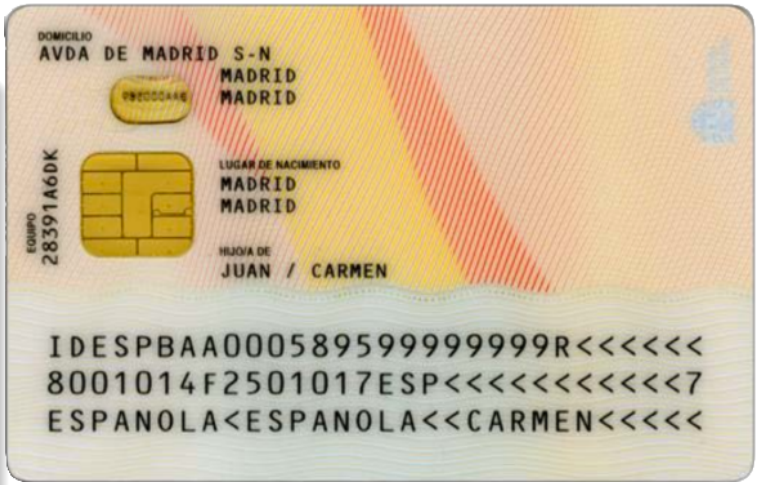
# Evolution of the Spanish Identity Card (DNI)

Book of Revelation (3)

## 2015–????

- **New number added in the front** (right-bottom corner)
- First DNIe3.0: Mireia Belmonte

**NFC capabilities**


## Some facts

- 6M of new DNIs issued per year (2014)
- **Myth Hunters**
  - **Last digit in second line of OCR is a control digit**
  - **DNI number is UNIQUE**

# Background on NFC

## What is NFC? – Near Field Communication

- **Bidirectional short-range contactless communication technology** ($\leq$ 10 cm)
- Based on RFID standards, works in the 13.56 MHz spectrum
- Data transfer rates vary: $106, 216$, and 424 kbps

# Background on NFC

## What is NFC? – Near Field Communication

- **Bidirectional short-range contactless communication technology** ($\leq$ 10 cm)
- Based on RFID standards, works in the 13.56 MHz spectrum
- Data transfer rates vary: $106, 216$, and 424 kbps

Security based on **proximity concern: physical constraints**

(remember: **not good**, as shown two years ago with Pepe ☺)

# Background on NFC

## What is NFC? – Near Field Communication

- **Bidirectional short-range contactless communication technology** ($\leq$ 10 cm)
- Based on RFID standards, works in the 13.56 MHz spectrum
- Data transfer rates vary: 106, 216, and 424 kbps

Security based on **proximity concern: physical constraints**

(remember: **not good**, as shown two years ago with Pepe ⌣̈)

## NFC-related ISO/IEC standards

- **ISO/IEC 14443**
  - Four-part international standard: Half-duplex communication, 106kbps
    - Two signalling schemes. DNIe3.0 follows Type-B scheme
  - **DNIe3.0 uses T = CL ISO-14443 as transmission protocol**
- **ISO/IEC 7816**: Fifteen-part international standard
  - **DNIe3.0 uses** $T = 0$ **ISO/IEC 7816**

# Agenda

# DNIe3.0 NFC Communication Protocols

NFC interface (1)

## Myth Facts

- **Monitor people during protests?** (http://www.elconfidencial.com/tecnologia/2015-01-16/identificar-a-distancia-con-el-nuevo-dni-3-0-la-n-de-nfc-significa-near_623075/)

# DNIe3.0 NFC Communication Protocols

NFC interface (1)

## Myth Facts

- **Monitor people during protests?** (http://www.elconfidencial.com/tecnologia/2015-01-16/identificar-a-distancia-con-el-nuevo-dni-3-0-la-n-de-nfc-significa-near_623075/)
  - **NO**. Best success probability $2.0833 \cdot 10^{-8} = \frac{1}{48 \cdot 10^6}$

# DNIe3.0 NFC Communication Protocols

NFC interface (1)

## Myth Facts

- **Monitor people during protests?** (http://www.elconfidencial.com/tecnologia/2015-01-16/identificar-a-distancia-con-el-nuevo-dni-3-0-la-n-de-nfc-significa-near_623075/)
  - **NO**. Best success probability $2.0833 \cdot 10^{-8} = \frac{1}{48 \cdot 10^6}$

## NFC security threats

- **Eavesdropping**
  - Secure communication as solution
- **Data modification** (i.e., alteration, insertion, or destruction)
  - Feasible in theory (but requires quite advanced RF knowledge)
- **Relays**
  - Forwarding of wireless communication

**Recommended lecture**: *Informe de Amenazas CCN-CERT IA-05/16*, CCN-CERT, 2016

# DNIe3.0 NFC Communication Protocols

NFC interface (2)

## Data divided in groups

- **Data Group 1**
  - Name and surnames: string
  - Nationality: string
  - Gender: string
  - No. of support: string
  - Expiry date: string
  - Birth date: string
  - Issuer: string (value “España”)
  - OptData: null
  - Document type: string (value “ID”)
- **Data Group 2**
  - **Facial photography** (JPEG2000 format, **no metadata**)
- **Data Group 7**
  - **Handwritten signature** (JPEG2000 format, **no metadata**)
- **Data Group 11**
  - Address: string
  - DNI number: string
  - Gender: string
  - Birth place: string (e.g., value “ZARAGOZA<ZARAGOZA”)
  - Title: null
  - **Telephone**: null
  - **Occupation**: null
  - CustodyInfo: null
  - ICAOName: null
  - OtherInfo: null
  - Summary: null

# DNIe3.0 NFC Communication Protocols

## Basic Access Control (BAC) protocol

- **ICAO Standard** (*Machine Readable Travel Documents - Part 11: Security Mechanisms for MRTDs*, 2015, `http://www.icao.int/publications/Documents/9303_p11_cons_en.pdf`)
  - **Defend against skimming and eavesdropping attacks**
- **Symmetric key device authentication**. After successful authentication, session key is agreed
- As initial key, some **parts of MRZ data**:
  - Serial number (3 alphabetic characters plus 6 digit)
  - Birth date (American format, “aammdd”)
  - Expiry date (American format, “aammdd”)

# DNIe3.0 NFC Communication Protocols

## Basic Access Control (BAC) protocol – analysis of entropy of key space

**Strength of the key depends on the strength of the MRZ-derived password** (symmetric cryptography)

- **Serial number**: $\log_2(26^3 + 10^6) = 34.0329$ bits
- **Birth date**: $\log_2(100 \cdot 365.25) = 15.1566$ bits
  - OSINT may reduce this value up to zero
- **Expiry date**: ($<$ 30yo, 5 years; 10 years, otherwise; no expiry date if $>$ 70yo)
  - $\log_2(10 \cdot 365.25) = 11.8347$ bits
  - Could be refined (e.g., only working days)

# DNIe3.0 NFC Communication Protocols

## Basic Access Control (BAC) protocol – analysis of entropy of key space

**Strength of the key depends on the strength of the MRZ-derived password** (symmetric cryptography)

- **Serial number**: $\log_2(26^3 + 10^6) = 34.0329$ bits
- **Birth date**: $\log_2(100 \cdot 365.25) = 15.1566$ bits
  - OSINT may reduce this value up to zero
- **Expiry date**: ($<$ 30yo, 5 years; 10 years, otherwise; no expiry date if $>$ 70yo)
  - $\log_2(10 \cdot 365.25) = 11.8347$ bits
  - Could be refined (e.g., only working days)


**$\approx$ 61 bits, less than the 80 bits recommended by both NIST and ECRYPT to protect against eavesdropping and other offline attacks**

# DNIe3.0 NFC Communication Protocols

## Password Authenticated Connection Establishment (PACE) protocol

- Advanced Security Mechanisms for Machine Readable Travel Document and eIDAS Token - Part 2, 2015, **BSI standard**

  (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile)

  - **Defend against offline attacks**
- **Generates cryptographically strong session keys from a weak password**
  1. The chip sends a random nonce encrypted with a password-derived key
  2. Mapping of the nonce to a random generator $\hat{G}$ of a group (e.g., an elliptic curve)
  3. Diffie-Hellman (DH) key agreement on the agreed-upon generator $\hat{G}$, and use the DH key to derive session keys
  4. Exchange and check authentication tokens

# DNIe3.0 NFC Communication Protocols

## Password Authenticated Connection Establishment (PACE) protocol

- Advanced Security Mechanisms for Machine Readable Travel Document and eIDAS Token - Part 2, 2015, **BSI standard**

  (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile)

  - **Defend against offline attacks**
- **Generates cryptographically strong session keys from a weak password**
  1. The chip sends a random nonce encrypted with a password-derived key
  2. Mapping of the nonce to a random generator $\hat{G}$ of a group (e.g., an elliptic curve)
  3. Diffie-Hellman (DH) key agreement on the agreed-upon generator $\hat{G}$, and use the DH key to derive session keys
  4. Exchange and check authentication tokens

- **Card Access Number (CAN)**
  - 6 digits
- $10^6 \rightarrow 2^{128}$
  - Sun $\rightarrow$ Alpha Centauri, $\approx 2^{45.18}$km

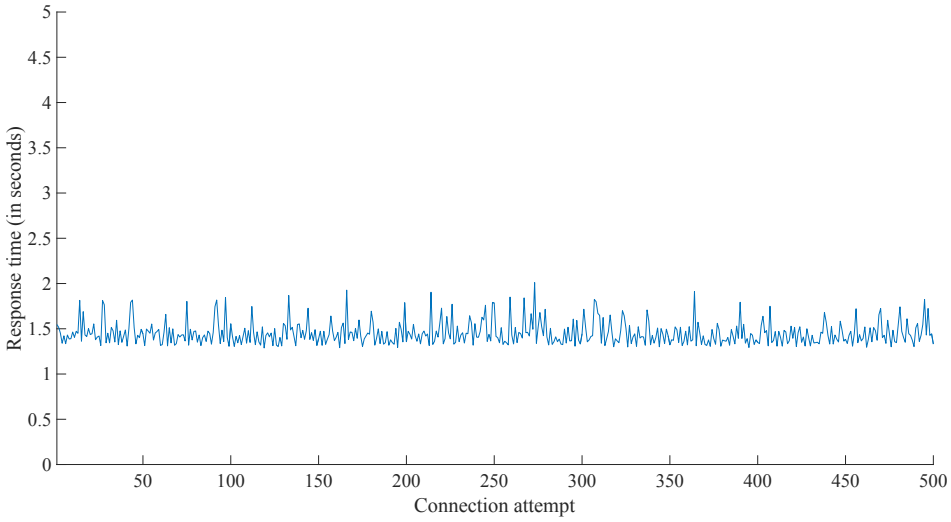
# Agenda

# Brute Forcing Password-Derived Keys

**How does the DNIe3.0 behave against a brute-force attack on the password-derived key used by the PACE protocol?**

- **Android app developed**, `AndroSmex` as code skeleton
- Hardware used:
  - SONY Xperia Z3 Tablet (2.5GHz, 3GB RAM, Broadcomm NFC chip)

- 500 connection attempts
- **On average, 1.4509 seconds**:
  - ≈ 200 ms to generate nonces
  - ≈ 1200 ms to perform DH protocol
  - ≈ 100 ms to generate, exchange, and check the authentication tokens



# Brute Forcing Password-Derived Keys

## Summary of findings

- **An incorrect CAN is only known in the last protocol step**
  - Authentication tokens mismatch and then connection is closed

# Brute Forcing Password-Derived Keys

## Summary of findings

- **An incorrect CAN is only known in the last protocol step**
  - Authentication tokens mismatch and then connection is closed

**GOOD!**
**No clue is given to a brute-force attacker**

- **No defense implemented against on-line brute-force attacks**
  - Execution time remains the same, regardless connection attempts

# Brute Forcing Password-Derived Keys

## Summary of findings

- **An incorrect CAN is only known in the last protocol step**
  - Authentication tokens mismatch and then connection is closed

**GOOD!**
**No clue is given to a brute-force attacker**

- **No defense implemented against on-line brute-force attacks**
  - Execution time remains the same, regardless connection attempts

**BAD! :(**

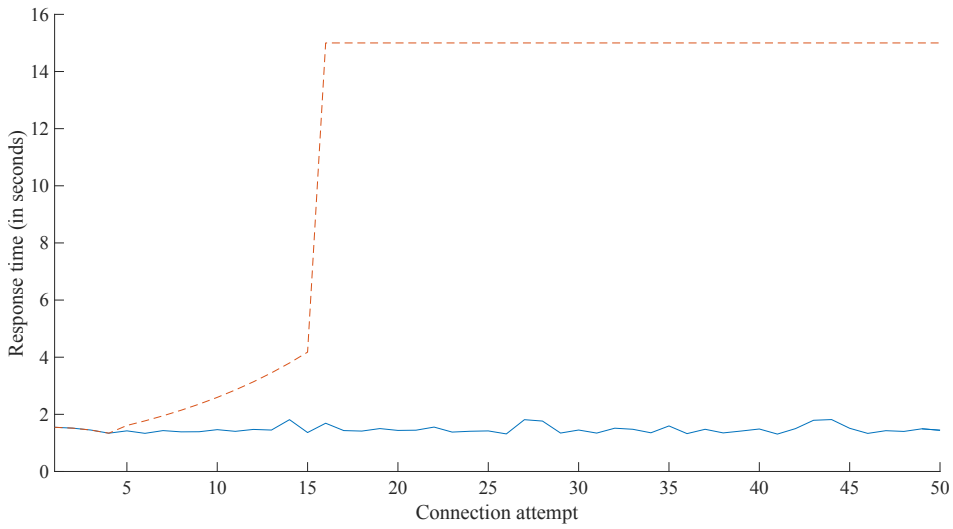
### Attack scenario (unlikely)

- **Android device compromised, detecting DNIe3.0 in NFC range**
- **17 days, in worst case** (assuming no interruption)
  - Persons of interest
  - Might be feasible also **if DNIe3.0 is fingerprinted** (stop/resume attack)

# Brute Forcing Password-Derived Keys

Improvement: adding a defense mechanism

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




- $i$: no. of connection attempt
- $t$: execution time
- Limits arbitrarily set to $[5, 15]$ (implementation decision)

**Acknowledged by the National Coinage & Stamp Factory – Royal Mint**

**To be considered for future DNIe3.0 implementation revisions**

# Randomness Analysis

**Is the pseudo-random number generator (PRNG) random enough?**

- Infineon SLE78CLFX408AP chip. **CC EAL5+ certification**
- **PRNG satisfies the requirements of class PTG.2 chip**, according to the BSI recommendation AIS 31 for physical RNGs
  - *The chip shall include a physical source of entropy, later fed into a software RNG. Output is then processed and checked for errors and statistical deviations*

## Experiment dataset and test suites

- $10^5$ **nonces collected from PACE connections**
- $2^{128}$ bits (16B)
  - **No repeated sequence (as expected)**
  - Probability of collision: order of $10^{-3}$ (loose birthday paradox estimation)
- Test suites: **compatible with our (relatively short) collection**

**This work was done in collaboration with J.C. García-Escartín, *University of Valladolid, Spain***

# Randomness Analysis

## ent utility

```
$ 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.
...
```

- **Entropy per byte is almost 8**
- **No appreciable size reduction with compression** (consistent with a random output)
- Pearson's $\chi^2$ test: results are as well within the **expected values for a random sequence**

# Randomness Analysis

FIPS 140-2 randomness tests (NIST) – `rngtest` from `rng-tools`

```
$  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
```

- Checks for expected probability of sequences of consecutive zeros and ones of different lengths (runs) and the frequency of fixed-size bit combinations
- **All tests passed with success**

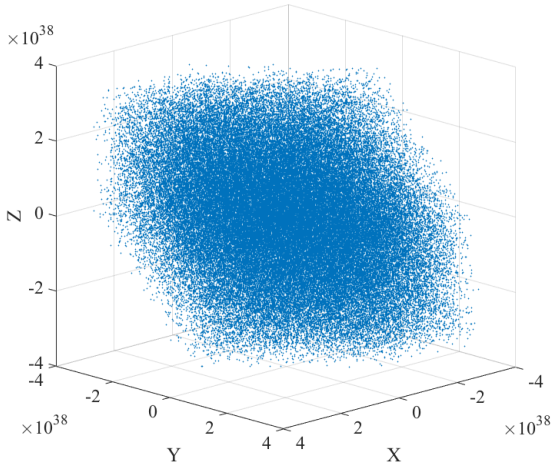
# Randomness Analysis

## Visual test – delayed coordinates method

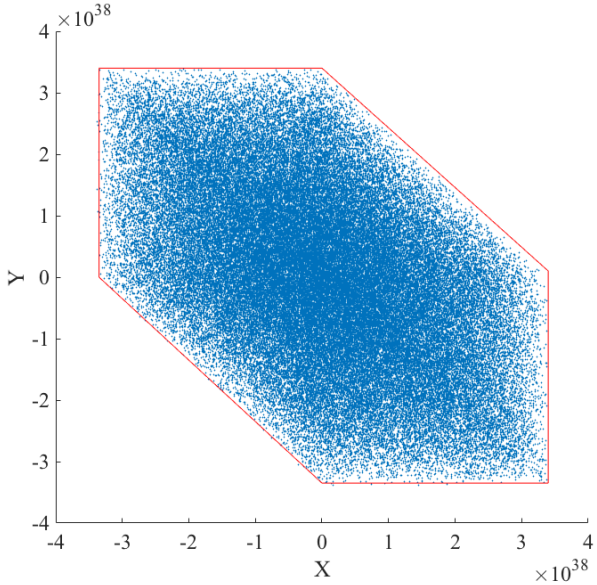
$$
\begin{aligned}
x(i) &= n(i) - n(i-1), \\
y(i) &= n(i-1) - n(i-2), \\
z(i) &= n(i-2) - n(i-3).
\end{aligned}
\tag{1}
$$

- Define **nonces as points in the phase space**
- If they are correlated, **we expect the points in the phase space to cluster in some attractor**

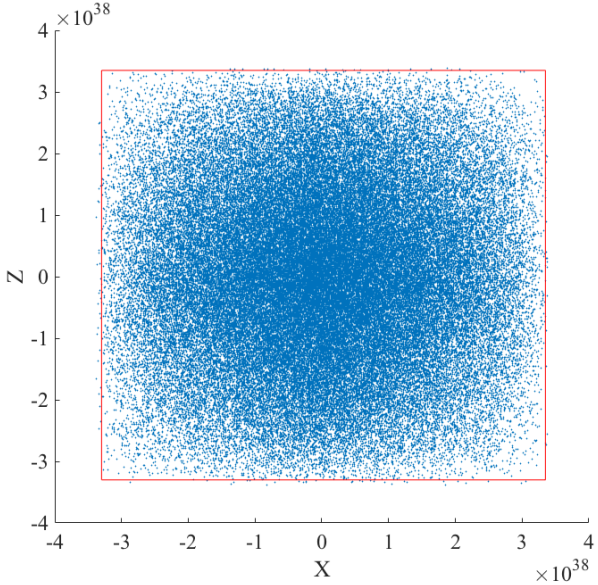
# Randomness Analysis



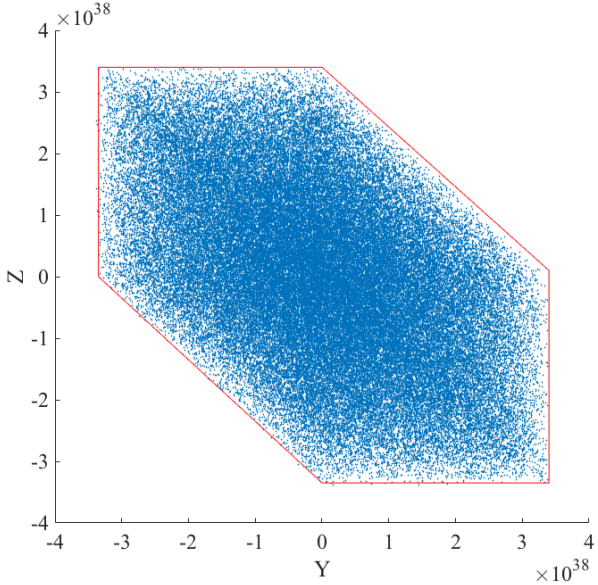

(a) *Delayed coordinates* 3D




(b) *Delayed coordinates* X-Y axes




(a) *Delayed coordinates* X-Z axes




(b) *Delayed coordinates* Y-Z axes

# Randomness Analysis

## Summary of findings

**The point distribution in the phase space is consistent with a uniform random number generator**

### DISCLAIMER

- **This test will not necessarily show long term correlations**
- However, considering also aforementioned experiment results, **our confidence on the *pure* randomness of the nonces is increased**

# Security Assessment

## DEMO


Source code available at `https://github.com/VictorSanchez94/DNIe3.0_brute_force_v2`

# Agenda

# Conclusions & Take-home message

- **DNIe3.0 incorporates a NFC chip: attack vectors increased**
  - Eavesdropping
    - Feasible, but data are ciphered
  - Data modification (i.e., alteration, insertion, or destruction)
    - Alteration/Insertion not possible (due to cryptography)
  - Relays
    - Not tested yet (although I would bet all-in on this)

# Conclusions & Take-home message

- **DNIe3.0 incorporates a NFC chip: attack vectors increased**
  - Eavesdropping
    - Feasible, but data are ciphered
  - Data modification (i.e., alteration, insertion, or destruction)
    - Alteration/Insertion not possible (due to cryptography)
  - Relays
    - Not tested yet (although I would bet all-in on this)

## Security assessment summary

- **Pseudo-random number generator**
  - **Pass several statistical test suites**
  - Random distribution fits into a perfect parallelepiped
- **PACE protocol is vulnerable**
  - **No defense implemented against online brute-force attacks**
  - Data accessed in 17 days, in worst case (assuming no interruption)

# Conclusions & Take-home message

- **DNIe3.0 incorporates a NFC chip: attack vectors increased**
  - Eavesdropping
    - Feasible, but data are ciphered
  - Data modification (i.e., alteration, insertion, or destruction)
    - Alteration/Insertion not possible (due to cryptography)
  - Relays
    - Not tested yet (although I would bet all-in on this)

## Security assessment summary

- **Pseudo-random number generator**
  - **Pass several statistical test suites**
  - Random distribution fits into a perfect parallelepiped
- **PACE protocol is vulnerable**
  - **No defense implemented against online brute-force attacks**
  - Data accessed in 17 days, in worst case (assuming no interruption)

**DNIe3.0 is secure enough** (at least for now)

# DNIe3.0 Security: More Problems Than Solutions?

Víctor Sánchez-Ballabriga[†], **Ricardo J. Rodríguez**[‡]

@RicardoJRdez ※ rjrodriguez@unizar.es ※ www.ricardojrodriguez.es





[†]Universidad de Zaragoza

[‡]Centro Universitario de la Defensa,
Academia General Militar (AGM)

March 04, 2017

**RootedCON 2017**
Madrid