ePassport: Securing International Contacts with Contactless Chips

Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater

Université catholique de Louvain
Louvain-la-Neuve, Belgium

Abstract. Electronic passports (ePassports) have known a wide and fast deployment all around the world since the International Civil Aviation Organization published their specifications in 2004. Based on an integrated circuit, ePassports are significantly more secure than their predecessors. Forging an ePassport is definitely thwarted by the use of cryptographic means. In spite of their undeniable benefit, ePassports have raised questions about personal data protection, since attacks on the basic access control mechanism came into sight. Keys used for that purpose derive from the nothing but predictable machine readable zone data, and so suffer from weak entropy. We provide an in-depth evaluation of the basic access key entropy, and prove that Belgian passport, recipient of Interpol "World's most secure passport" award in 2003, provides the worst basic access key entropy one has ever seen. We also state that two-thirds of Belgian ePassports in circulation do not implement any data protection mechanism. We demonstrate our claims by means of practical attacks. We then provide recommendations to amend the ePassport security, and directions for further work.

1 Introduction

Malaysia was the first country in the world to issue electronic passports. It adopted this technology in March 1998, thus predating the standard [13, 14], aka Doc. 9303, elaborated by the *International Civil Aviation Organization* (ICAO). Belgium was the first country worldwide[1] to issue ICAO-compliant electronic passports (ePassports). Nowadays, more than 50 countries issue ePassports, for example USA, UK, Germany, France, Italy, Belgium, Australia, Singapore, Switzerland, etc.

The wide and fast deployment of ePassports has mainly been possible thanks to the ICAO efforts. In 1997, the ICAO commenced a comprehensive revision of its documents, and disclosed the first versions of ePassport specifications in 2004. The US Visa Waiver Program[2] has also considerably accelerated this wide spread. It enables citizens from about 27 countries to travel to the USA for

[1] `http://judiciary.house.gov/OversightTestimony.aspx?ID=352`
[2] `http://travel.state.gov/visa/`

tourism or business for stays of 90 days or less without obtaining a visa. However, countries were required to have an ePassport issuing system in place by 26 October 2006, in order to continue as members of the program.

An ePassport (or biometric passport) is the same as a traditional passport combined with an *integrated circuit* (IC) embedded either in its cover pages or laminated over a data page. According to the ICAO, the IC must store as a minimum the duplicate of the *Machine Readable Zone* (MRZ) and a digital facial image of the passport's holder. The MRZ is the two optically readable encoded lines at the bottom of the passport first data page and includes the document type, full name, passport number, nationality, date of birth, gender, date of expiry, and the corresponding check digits. The IC may also contain lots of optional information such as handwritten signature, fingerprints, address, phone numbers, information about the persons to notify in case of emergency, etc.

Data stored in the IC is digitally signed by the issuing country using a highly protected private key. Consequently, one cannot modify or create from scratch a passport without being detected. Equipped with sufficient storage memory, the ePassport allows incorporating biometrics that add additional identification features, that is the name "biometric passport". Consequently, information stored in the IC, information available from the *Visual Inspection Zone*[3] (VIZ), and biometrics of the physical person can be compared. Finally, the IC may optionally prevent cloning or substitution since it has the ability to prove the possession of an asymmetric private key. A contactless or RFID (*Radio-Frequency Identification*) technology has been chosen due to its numerous advantages compared to the contact-based one. Incorporating the IC into the passport book is much easier and the inspection process becomes very handy. In particular, using this technology does not require to position the passport accurately on the reader.

However, based on a contactless technology, this IC has created many new security threats [1, 2]. Juels, Molnar, and Wagner [17] explored some of these threats in the context of the US passport. They mainly discussed the data leakage and biometric threats. Besides, they discussed the *Basic Access Control* (BAC) low entropy of the US passport. Kc and Karger [18] rewrote this work and discussed additional issues related to slice attacks (encountered in hotels and banks), fake fingers, and the BSI proposal for *Extended Access Control* (EAC). Hoepman *et al.* [12] discussed particularly the BAC in the context of Dutch passport, traceability, EAC, and threats of ePassport-based new applications. Monnerat, Vaudenay, and Vuagnoux [21] reviewed the ePassport privacy issues, and focused on the *Active Authentication* side effects. They proposed a GQ-based authentication protocol as a possible countermeasure. Lehtonen *et al.* [20] proposed combining RFID with optical memory devices in order to improve the security of machine readable documents. Witteman [27] established a practical attack against the BAC of the Dutch passport. Grunwald executed a similar attack on the German ePassport [7]. Laurie also successfully cloned a UK ePassport while it was hidden in an envelope [19]. All of them, however, assume some

[3] Information on the passport's first data page.

known information about the passport's owner. Recently, Halváč and Rosa [11] investigated the feasibility of performing a relay attack on Czech ePassport, and finally Ortiz-Yepes [22] supplied a short overview of security mechanisms recommended by ICAO.

In this work we go one step forward, proving that the real entropy of the BAC keys is much lower than what is stated in the previous analyzed passports. We operate a practical attack against the Belgian ePassport, and reveal that two-thirds of Belgian ePassports do not implement the BAC, which conflicts with the claims of the Belgian Minister for Foreign Affairs who declared in the Parliament [8] that Belgian ePassport benefits from the BAC. We then point out some further weaknesses, and provide heuristics that allow an adversary to guess the issuing country of a given passport while she is not able to pass the BAC. Finally, we present recommendations to enforce security in ePassports.

The remaining of this article is organized as follows. Section 2 provides a comprehensive introduction to the ICAO algorithms. Weaknesses in ICAO standard and practical attacks are presented in Section 3, and recommendations to improve ePassport security are presented in Section 4. Finally, Section 5 concludes our work.

2 ICAO Standard

ICAO began working on machine readable travel documents in 1968, in the interest of securing passports and accelerating the clearance of passengers. The MRZ concept was introduced in 1980 in Doc. 9303, published as "A Passport with Machine Readable Capability". That is only in 2004 that ICAO introduced a new direction in Doc. 9303, requiring passports to embed an electronic chip, an idea already suggested by Davida and Desmedt [4] in the eighties.

2.1 Embedded IC Specifications

The ICAO specifies that ICs are to conform to ISO/IEC 14443 Type A or Type B [16] and the onboard operating system shall conform to ISO/IEC 7816-4. The main difference between Type A and Type B is the modulation of the RF signals. As a consequence, the collision avoidance protocols are also different. In the world, Type A and Type B conforming ePassports are respectively 64% and 36% according to [26]. ISO/IEC 14443 also specifies that the reading range should be less than 10 cm (security feature), the frequency is 13.56 MHz, and the ICs are passive (power derived from the reader). Finally, the data storage capacity of the IC must be at least 32 kB in order to store the mandatory facial image and duplication of the MRZ data, but the common size is 70 kB. Besides, the passport chip contains a microprocessor with a coprocessor for the cryptographic functions in order to be able to use evolved cryptographic functions.

2.2 Data on the IC

First of all, to ensure global interoperability of ePassports, Doc. 9303 specifies a *Logical Data Structure* (LDS) compliant to ISO-7816. This LDS consists of 2 mandatory *Data Group*, DG1 and DG2, that respectively contain the facial image and a copy of the MRZ. It also consists of 17 optional DGs. For example, a handwritten signature may be stored in DG7 and DG15 is reserved for active authentication. Data groups DG17 to DG19 are reserved for future use to store electronic visa, automated border clearance, and travel record.

The IC also stores a file EF.COM that contains common information for the application, especially the list of DGs present on the IC. It stores as well a file named EF.SOD (*Document Security Object*) that contains security data that will be detailed later in this paper. Finally, the IC contains additional information whose storage and access are left to the developer discretion [6] (not accessible through the ICAO-standardized interface): BAC keys, active authentication private key, application identifier, life cycle status, etc.

2.3 Biometrics

Representing something you are, biometrics are used to identify uniquely a human being through the measurement of distinguishing physiological (face, fingerprint, iris, DNA) or behavioral (signature, keystroke dynamics, voice) characteristics. Biometrics can improve the security of the inspection process by increasing the strength of the link between the travel document and its owner. The ICAO only favored and classified three types of biometrics: face, fingerprint, and iris recognition. The facial image is not considered by the ICAO as sensitive (not confidential) information, contrarily to fingerprints and iris. The passport does not record a template of the biometrics, but a picture (JPEG or JPEG2000), enabling countries to choose their preferred facial recognition system.

2.4 Cryptographic Mechanisms

The ICAO has specified countermeasures to fulfill the ePassport security requirements. *Passive Authentication* proves that the passports content has not been modified. *Basic Access Control* (BAC) guarantees that the passport is open willingly and that the communication with the reader is secure. *Active Authentication* is to prevent chip cloning, and finally *Extended Access Control* (EAC) is to protect the confidentiality of additional biometrics.

Passive Authentication. The only countermeasure required by the ICAO is that data stored on the passport's IC be digitally signed by the issuing country in order to prevent data modification. To do so, each DG of the LDS is hashed using SHA-1 and all theses hashes together are signed by the *Document Signer Private Key*. The signature is stored in the IC's EF.SOD. Any inspection system needs the *Document Signer Public Key* to verify the LDS integrity. The appropriate certificate can be found either in the IC (EF.SOD) or from the ICAO

dedicated repository accessible only for participants. The document signer public key certificate is in turn signed by the *Country Signing Private Key* and can be checked using a root certificate that is spread by diplomatic means.

Basic Access Control. In skimming the adversary queries the passport (without holder's consent), while in eavesdropping she passively intercepts communications between the reader and the passport. The ICAO recommends the BAC mechanism as a countermeasure against skimming and eavesdropping by (1) authenticating the reader and (2) encrypting the communication.

Authenticating the reader. When BAC is supported, the reader cannot get any information from the passport unless it goes through a challenge-response protocol (Fig. 1) based on the cryptographic functions here denoted ENC[4] and MAC[5]. In this protocol, C_P and C_R are two 8-byte random challenges respectively generated by the passport and the reader, and K_P and K_R are two 16-byte random values, again respectively generated by the passport and the reader. With this protocol, the reader proves to the passport the knowledge of the BAC keys (K_{ENC} and K_{MAC}) that are derived from some information of the MRZ (date of birth, date of expiry, and passport number) using SHA-1 (See Doc. 9303 for the description of the key derivation procedure). The exchanged values K_P and K_R are used afterwards by the reader and the ePassport to agree on session keys KS_{ENC} and KS_{MAC} for securing the communication. Note that this protocol does not ensure strong authentication. Instead it is intended to prove that the person has willingly opened his passport: anyone who knows the MRZ can successfully be authenticated. In other terms, the goal of BAC is to mitigate the security issue arisen from the contactless technology.

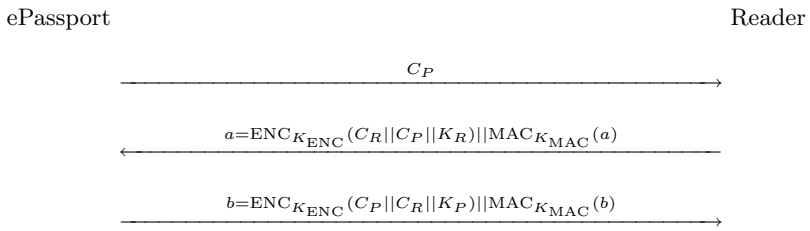

Fig. 1. Basic Access Control

Encrypting the communication. After successful execution of BAC, both the reader and the IC compute session keys, KS_{ENC} and KS_{MAC}. Session keys are generated using the same key derivation procedure used for BAC keys but ($K_P \oplus K_R$) is used as seed instead of the hash of birth date, date of expiry, and passport number. These keys are used to encrypt all the subsequent communications

[4] ISO/IEC 11568-2, 3DES, CBC mode, zero IV (8 bytes).
[5] ISO/IEC 9797-1, MAC Algorithm 3, block cipher DES, zero IV, Padding Mode 2.

using again the cryptographic functions ENC and MAC defined above. This mechanism, known as *secure messaging*, provides confidentiality and integrity of the communication between the inspection system and the ePassport.

Active Authentication. BAC and Passive Authentication do not prevent chip cloning or substituting, an attack that may be particularly attractive in unattended identification systems[6]. Active Authentication is recommended to prevent these attacks using a challenge-response protocol in which the passport proves the possession of a private key. This private key is stored in a secure memory while the corresponding public key is stored in DG15. The procedure, which is depicted in Fig. 2, is that the reader sends a challenge C_R to the passport that signs it, and sends the signature back to the reader, which verifies it using the public key.

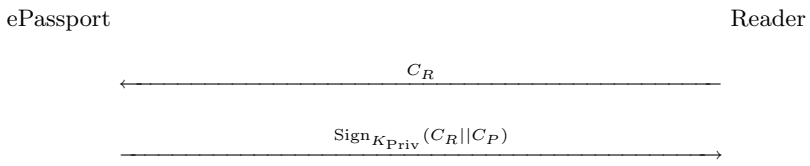

Fig. 2. Active Authentication

Extended Access Control. The ICAO has recommended EAC to guarantee the confidentiality of additional sensitive biometrics (fingerprint, iris) but it has not standardized any EAC protocol yet. The European Union pioneered this mechanism, and released a first version early in 2006 [24]. Security of EAC is still a work in progress, and several flaws have already been pointed out in [12, 21].

3 Guessing the BAC Keys

The BAC is founded on the philosophy that it cannot be passed unless the passport was willingly opened. This is not the case in practice since the BAC keys are derived from the easy-to-get MRZ information. Below, we describe the theoretical entropy and show that it really differs from the practical one.

3.1 Theoretical Entropy

Doc. 9303 [14] defines the structure of the date of birth as YYMMDD, implying an entropy of $\log_2(100 \times 365.25) \approx 15$. The date of expiry provides

[6] Automated border controls are already in use in airports, e.g., in Frankfurt, Paris, Amsterdam, and Sydney.

$\log_2(10 \times 365.25) \approx 12$ bits when the validity period is 10 years [14]. Only the first 9 characters of the passport number are involved to generate the BAC keys. Consequently, the relative entropy is $\log_2((26+10)^9) \approx 46$, leading to 73 bits in total. Unfortunately, the effective entropy is much lower. The ICAO itself estimates it to 56 bits, due to the weak passport numbering schemes.

3.2 Effective Entropy

Doc. 9303 is flexible to take account the regulations of each participant. Especially, countries all have their own numbering schemes. US passport number consists of 9 digits where the first two digits are used to encode one of the 15 passport issuing agencies [17]. Thus, the entropy of this field decreases to $\log_2(15 \times 10^7) \approx 27$ and the total entropy becomes 54 at best.

German passport number consists of 9 digits where the first 4 digits are attributed to 5 700 local passport offices (in 16 Federal States) [5] and the remaining 5 digits for a serial number [3], so its entropy is $\log_2(5700 \times 10^5) \approx 29$. For 5-year passports, the total entropy is so 55 bits. Carluccio *et al.* [3] estimates it to 40 as realistic value, but they do not provide any explanation.

In the Netherlands, the passport number consists of a static letter "N" combined with 8-digit sequential number [23] and the passport is valid for 5 years. Moreover, the last digit is a predictable check digit [23, 27], reducing the total entropy to 50 bits according to Hoepman *et al.* [12]. They also report that this entropy can be reduced to 41 under certain assumptions (e.g., age can be guessed within a margin of 5 years).

In our case, that is the Belgian passport, the situation does not look worse: the passport number consists of 2-letter prefix and 6-digit suffix, providing an entropy of $\log_2(26^2 \times 10^6) \approx 29$ bits. Passports being valid during 5 years, the overall entropy is about 54 bits. The Belgian passport entropy is so fairly comparable to those of other countries. Unfortunately, our thorough analysis of the Belgian passport numbering scheme points out serious weaknesses. The main weakness is that numbers are chosen sequentially during the passport book *manufacturing* phase. Each blank passport has its unique identifier that becomes the passport number assigned during the *personalization* phase. Thus, there is a strong correlation between the date of issue (and so the date of expiry) and the passport number. For that reason, anyone can *roughly* guess the number of a passport given its issue date (or, equivalently, its date of expiry), that is to say, anyone is able to specify a range of passport numbers the target belongs to. The exact passport number cannot be guessed because (1) several thousand passports are issued every day; (2) the flow of issued passports is not constant and depends on several (more or less) predictable events, e.g., more passports are issued before the vacated months; (3) passports are not issued in exactly the same order as they have been manufactured, for some unclear logistic reasons. Consequently, given three pairs (d, n), (d', n'), and (d'', n''), where d, d', and d'' are three issue dates and n, n', and n'' are three passport numbers:

$$d \leq d' \leq d'' \not\Rightarrow n \leq n' \leq n''.$$

However, the observation of several pairs (issue date, passport number) allows calculating a value δ such that, for most of the passports:

$$d \leq d' \leq d'' \Rightarrow n - \delta \leq n' \leq n'' + \delta.$$

We recorded many Belgian passport numbers and respective issue dates. Each observed pair is represented by a cross in Fig. 3. On a given segment (the segmentation-effect will be explained later), the cross are not straight aligned due to the three above reasons. However, given an issue date of a targeted passport, it is possible to approximate its number with precision $\pm\delta$, and δ becomes tighter while new pairs of passport numbers and issue dates are recorded. Theoretically, 2δ can drop down to the number of daily-issued passports. That is however a theoretical bound that cannot be reached in practice due to reasons (2) and (3) stated above. Another reason is that some numbers are never assigned to blank passports, leaving some holes in the sequential numbering, in order to help detection of fake passports. In our case, we reached $\delta = 12\,000$ after only 40 observations, while about one thousand passports are issued every working day. One important phenomena in Fig. 3 is the segmentation-effect. These jumps in the numbering are due to a Belgian particularity: Belgium has several official languages, namely French, Dutch, and German. A Belgian citizen receives a passport such that its "reference" language is the one of the area he lives in or the one of his choice (ability to choose one's reference language is only available in a few bilingual areas, e.g., Brussels). This reference language does not only influence the personalization stage, but also the manufacturing process. Indeed, the passport cover and the on-page pre-printed information depends on the reference language. Consequently, the manufacturer provides language-dependent batches of blank passports to the authorities.

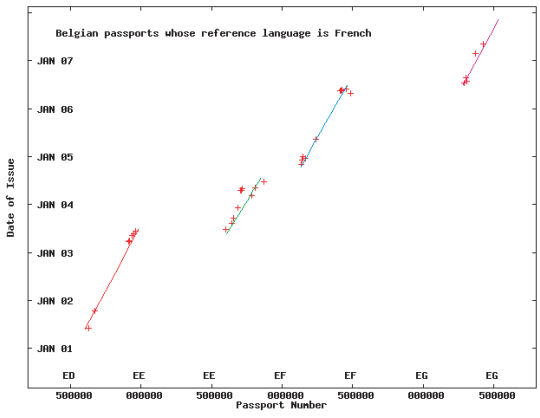

Fig. 3. Distribution of Belgian Passport Numbers

Figure 3 represents only passports whose reference language is French. The jumps correspond to the two other official languages. So, given the living place or the preferred language of a person, guessing his passport number[7] becomes much easier using the appropriate approximation.

Last but not least, ePassports are not issued during week-ends and holidays in Belgium, like in many other countries, meaning that ePassports are issued roughly 250 days a year. Using all these heuristics, the entropy of the passport becomes $\log_2((250 \times 5) \times (100 \times 365.25) \times 2\delta) \approx 40$ bits, and the entropy still drops down with every new-known combination of passport number and date of expiry. Finally, second-generation Belgian passports have been issued since mid 2006 only and so the range of issue dates is today quarter of the theoretical range. This means that the entropy of todays Belgian passport is about 38 bits. Note that in case an adversary has a targeted victim, it is realistic to assume that his date of birth is known. This assumption, which is commonly done in the previous works, still lowers the entropy down to 23 bits (See Tab. 1).

Table 1. Effective Entropies of Selected Countries

Country	**Effective**	**Birth date known**
Germany [3]	55	40
USA [17]	54	39
Netherlands [23]	50	35
Belgium	38	23

3.3 Our Practical Attacks Against Belgian Passport

In this section, practical attack means successful reading of passport's digital content. In fact, two types of attacks can be distinguished, on-line and off-line. Off-line attack is when an adversary eavesdrops the communication, and later recovers the BAC keys by brute-force. On-line attack is trying to brute-force the keys in real time, by skimming.

On-line attack. This attack is definitely the most difficult to carry out due to (1) the response time of the IC and (2) the communication rate, which is between 106 kbit/s and 848 kbit/s according to ISO 14443.

Our equipment (low-cost reader that can reach 115 kbit/s baud, rather old laptop, and non-optimized implementation of Doc. 9303) was able to query the IC 400 times per minute. This is far below the limits. A high-performance system should be able to carry out few thousands queries per minute.

Using our heuristics, recovering the BAC keys should take a few weeks with our pretty non-optimal material, assuming only the date of birth is known (the

[7] We did not consider official passports, as diplomatic, service, or politician passports.

issue date and passport number are not known). However, Sec. 3.2 considers that, for a given issue date, the passport number is uniformly distributed in a set of size 2δ, while this is not the case in practice. 2δ is the worst case for most of the passports, but a clever exhaustive search significantly decreases the cryptanalysis time: for a checked issue date, the cracking program looks for the corresponding expected passport number on the segment (Fig. 3), and tries every passport number from this point by positive and negative incremental steps.

Consequently, the average cryptanalysis time is far below the theoretical value. For instance, the last passport we cracked was issued on July 2007 (day not disclosed for security reason) and the corresponding passport number approximated by our program was EG473598, which was only about 4 000 numbers below the real value.

Off-line Attack. Off-line attacks are much more efficient. However, while on-line attacks use the passport as an oracle to test every BAC keys, off-line attacks require a ciphertext as material for the attack. Such a ciphertext is not provided by the IC till the BAC protocol succeeds. This means that an off-line attack is only possible if the adversary is able to eavesdrop a communication between a passport and a reader. Today, passports may be only read by immigration and police officers. However, tomorrow, they will be read by officer in banks, hotels, airlines companies, etc., and it will so become much easier to eavesdrop communications. With an entropy of 23 bits, carrying out an off-line attack takes about one second with any today's PC. An interesting point is that in the BAC protocol (Fig. 1), both messages $a = \mathrm{ENC}_{K_{\mathrm{ENC}}}(C_R||C_P||K_R)||\mathrm{MAC}_{K_{\mathrm{MAC}}}(a)$ (reader-to-passport message) and $b = \mathrm{ENC}_{K_{\mathrm{ENC}}}(C_P||C_R||K_P)||\mathrm{MAC}_{K_{\mathrm{MAC}}}(b)$ (passport-to-reader message) can be used as support of the off-line attack. Given that the reader-to-passport communication can be eavesdropped at a much larger distance than the passport-to-reader communication, an off-line attack does not require to be close to be performed. Of course, the adversary will have to approach the ePassport afterwards to download its content.

The Most Efficient Attack. Surprisingly, our attack initially failed when we sent to the first-experimented ePassport the command `GET_CHALLENGE`, which is required to execute the BAC. This failure meant that the interrogated ePassport was not able to generate the pseudo-random number C_P required in the first message of the BAC protocol (Fig. 1). Further investigations have shown that it did not implement BAC. In other words, the personal data were not protected. It turns out that Belgian ePassports are divided into two generations. The first generation that comprises passports issued from end 2004 till mid 2006 do not support BAC. Second generation passports have been issued since mid 2006 and implement BAC. Reading the content of a first generation passport (without the owner's knowledge) is obviously very simple since no authentication is required. A few seconds were needed with our low-performance system to download all the information from the passport. We put our attack into practice using a reader and a laptop hidden in an attaché-case.

Today[8], two-thirds of Belgian ePassports in circulation are 1st generation passports and some of these non-protected passports are valid until 2011. More precisely, there exist 1 500 000 valid Belgian passports in circulation. Among them, 430 000 are former non-electronic passports, 720 000 are 1st generation ePassports, and 350 000 are 2nd generation ePassports. Diplomats in some countries were among the first citizens to receive ePassports. It is so highly unlucky that Belgian diplomats hold or held 1st generation ePassports.

4 Recommendations

Ensuring that an adversary cannot impersonate someone else is a matter of the utmost importance. Ensuring that she cannot steal personal data is also a major concern. One may say that personal data available on an ePassport IC is nothing more than MRZ and VIZ. That is today's truth, but fingerprints and perhaps additional data will also be stored in ePassport ICs in the near future. Furthermore, even the remote disclosure of MRZ and VIZ can be felt as an intrusion in our personal lives. This theft can be done without the ePassport holders awareness, and stolen data can be used for further malicious exploits. For example, the Belgian passport stores, in addition to the mandatory data (DG1 and DG2), some optional data (DG7: handwritten signature; DG11: birth place and date; DG12: issue place and date). The passport does not record templates of the biometrics, but JPEG images. While today signed faxes or signed PDF files are accepted as an alternative to signed physical documents, the picture quality of the handwritten signature is good enough (800×265 pixels) to forge a fake fax or PDF file. Below, we provide recommendations and countermeasures to enforce security in ePassport. Some of them require modifications of the ICAO standard while some others only need modifications of the countries policy.

4.1 Delaying IC Answers

As we saw in the previous sections, one important security issue comes from skimming attacks. One possible way to thwart or mitigate these attacks is to delay the IC responses when several queries are received in a short period of time. If the response delay is progressively increased and upper-bounded, this protection cannot open the way to denial-of-service attacks. We know that this technique already exists but it is definitely not implemented on ePassport ICs. We do not see any technical issue to the implementation of such a protection in ePassports.

4.2 Random Passport Numbers

We have shown that the BAC keys suffer from very low entropy. In the Belgian case, the entropy can drop down to 23 bits if the date of birth is known. This

[8] Mid 2007.

issue can be mitigated without modifying the ICAO standard. Indeed, instead of using a deterministic passport numbering scheme, passport numbers should cover the full potential of ICAO standard. In other words, passport numbers should be randomly picked in $\{A-Z, 0-9\}^9$. The total entropy in that case would be about 57 bits when the date of birth is known and 73 otherwise (assuming passports are issued only 250 days a year).

To illustrate our recommendation, consider that an adversary writes down on the ground all the passport numbers she should check for each (issue date / date of birth) pair to break the BAC keys. Assuming that she is capable of writing one passport number every millimeter, she will have to walk 25 000 times around the World (along the equator) if the passport numbering scheme exploits the full passport number space. Using our (Evil) heuristics, writing Belgian passport numbers requires today walking only 24 meters. This clearly shows that using the full space of passport numbers is fundamental.

Using random passport numbers increases the entropy of the BAC keys up to 73 bits, but this remains insufficient, especially when the adversary knows some information, e.g., date of birth or date of expiry. This problem can be solved by modifying ICAO standard: BAC key generation should be randomized. Since there exists an optional 14-character field in the MRZ (whose purpose is at the discretion of the issuing countries, but usually never used), putting randomness in this field can be performed without modifying the MRZ structure.

4.3 Separate BAC Keys and Personal Data

Improving the effective entropy of BAC keys reduces the risk of remote access to the the ePassport without agreement of its holder. However this solution does not prevent inadvertent disclosure of BAC keys, e.g., in hotels, car rental shops, exchange office, etc. as they usually require a copy of the VIZ. Personal data are then digitalized and stored in databases, and they are eventually disclosed. The fundamental issue is that BAC keys are directly generated from the MRZ (and so from the VIZ). One way to avoid disclosure of the BAC keys is to generate them from random material that does not belong neither to the VIZ, nor to the MRZ. When the passport is shown up, and possibly photocopied for archives, the random material is not revealed if it is not printed on the same page as the VIZ. It can be printed on another page of the passport, e.g., on the last page in order to fasten the inspection, or it can be made available on another support (optically or electronically readable), e.g., a plastic card. This card should only be shown up to inspection officers.

4.4 Radio-blocking Shield

Protecting personal data can be enforced using strongest BAC keys. Another palliative way to avoid IC access without the holder's awareness is to insert a radio-blocking shield in its cover, as it is done in the US passport. With such a shield, nobody can read a passport while it is closed. Surprisingly, this technique

is only used in the US passport, up to our knowledge. We recommend to widely deploy this radio-blocking shield integrated in the cover.

4.5 Active Authentication

Active Authentication may allow an adversary to force an ePassport to sign some value [14]. Indeed, as depicted in Fig. 2, the adversary sends a value C_R she chose herself and the ePassport answers with $\text{Sign}_{K_{\text{Priv}}}(C_R||C_P)$, where C_P is a random value chosen by the passport. Sending an appropriate C_R, e.g., result of the lottery, an adversary can build a proof that the considered passport has been seen after a given date (she is then able to show this proof up in court). As suggested by Vaudenay and Vuagnoux in [25], a signature scheme without proof-transferability should be used instead of the current protocol. Later on, Monnerat, Vaudenay, and Vuagnoux [21] suggested a solution based on Guillou-Quisquater [9, 10] identification scheme. We consider that implementing a signature scheme that does not allow proof-transferability would constitute a step forward in securing ePassports. Our statement is also based on the fact that ePassports may also serve to secure external applications. In that direction, ICAO published a request for information [15] on the future specification development related to ePassport. Among the topics of interest, one could point out the category *Data chip partitioning* that concerns "effective methodology for securely partitioning data on e-Passport chips to allow for data and / or functions to be added by third parties"; and the category E-Commerce that deals with "electronic on-line systems that may be applied to secure Internet based passport and visa application processes".

4.6 Favorite Algorithms

Giving countries the ability to choose the BAC key generation procedure leads to weaknesses. Choice of other algorithms is also left to the discretion of the countries, although they must belong to a given cryptographic toolbox defined by ICAO. Unexpected security level may appear in case of non-appropriate choice. For instance, Tab. 2 and Tab. 3 show that Belgian ePassport uses SHA-1, which is not recommended, and absolutely not appropriate to be used with RSA-2048 and RSA-4096.

5 Conclusion

The ePassport is the most secure international identification document ever seen. It guarantees information integrity, authenticity, and confidentiality, based on well-known cryptographic tools. Security and safety are more than ever enforced by means of biometrics. Deploying a wide-range international trustful PKI was a prerequisite for this achievement. By doing so, the ICAO afforded to the ePassport a promising future in many domains as banking and trading to name a few. Nevertheless, some security and privacy issues still exist and must be addressed.

Table 2. ICAO-compliant Algorithms and Belgian Case

Algorithm	ICAO	Belgian ePassport
BAC (incl. secure messaging)	3DES/CBC Retail-MAC/DES	3DES/CBC Retail-MAC/DES
Hash for key derivation	SHA-1	SHA-1
Hash for signature	SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512	SHA-1
Signature	RSA-PSS, RSA-PKCS1-v15, DSA, ECDSA (X9.62)	RSA-4096 (Country Signing Key), RSA-2048 (Document Signer Key), RSA-1024 (Active Auth.)

* ICAO [14] recommends not to use SHA-1 whenever hash collisions are of concern.

Table 3. ICAO Recommended Security Levels and Security Equivalence

Purpose	Security level	RSA modulus n	DSA modulus p,q	ECDSA base point ord	Hash function
Country Signing CA	128	3072	3072, 256	256	SHA-256
Document Signer	112	2048	2048, 224	224	SHA-224
Active Authentication	80	1024	1024, 160	160	SHA-1

Sizes are expressed in bits.

Among them, the entropy of the BAC keys, which ensure privacy-protection, is not sufficient. We provided in this paper a thorough analysis of this issue and presented our investigations on the Belgian ePassport. We proved that the entropy can be as low as 23 bits under certain assumptions, and we revealed that two-thirds Belgian ePassports in circulation have no concern with privacy-protection. We then provided comprehensive security recommendations, for guiding countries in defining their policies and for amending future releases of Doc. 9303.

Acknowledgments

We would like to kindly thank people who helped us during this work. Among them, Danny De Cock and Elke Demulder for fruitful discussions about Belgian ePassport, and Serge Vaudenay and Martin Vuagnoux for providing us helpful information.

References

[1] G. Avoine. *Cryptography in Radio Frequency Identification and Fair Exchange Protocols.* PhD thesis, EPFL, Lausanne, Switzerland, December 2005.
[2] G. Avoine. Bibliography on security and privacy in RFID systems. Available Online, 2007.
[3] D. Carluccio, K. Lemke-Rust, C. Paar, and A.-R. Sadeghi. E-Passport: The Global Traceability Or How to Feel Like a UPS Package. Workshop on RFID Security, July 2006.

[4] G. Davida and Y. Desmedt. Passports and Visas Versus IDs. In *Advances in Cryptology – EUROCRYPT'88*, LNCS, May 1988.
[5] E. Friedrich. The Introduction of German Electronic Passports. Second Symposium on ICAO-Standard, MRTDs, Biometrics and Security, September 2006.
[6] Gemalto. e-Passport AXSEAL CC V2 36K – Common Criteria / ISO15408 EAL4+ – Security Target. Technical report, Gemalto, 2004.
[7] L. Grunwald. New Attacks against RFID-Systems. GmbH Germany.
[8] K. D. Gucht. Chambre des représentants de Belgique, compte rendu intégral avec compte rendu analytique traduit des interventions. Commission des relations extérieures, 2007.
[9] L. Guillou and J.-J. Quisquater. A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge. In C. Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *LNCS*. Springer-Verlag, August 1988.
[10] L. Guillou and J.-J. Quisquater. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Trasmission and Memory. In *Advances in Cryptology – EUROCRYPT'88*, LNCS. Springer-Verlag, May 1988.
[11] M. Halváč and T. Rosa. A Note on the Relay Attacks on e-passports: The Case of Czech e-passports. Cryptology ePrint Archive, Report 2007/244, 2007.
[12] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. W. Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In *Advances in Information and Computer Security*, LNCS. Springer-Verlag, 2006.
[13] ICAO. Machine Readable Travel Documents. Technical report, ICAO, July 20 2005. Doc 9303 Part 1 Volume 1, 10th Draft, Sixth Edition.
[14] ICAO. Machine Readable Travel Documents. Technical report, ICAO, July 20 2005. Doc 9303 Part 1 Volume 2, 9th Draft.
[15] ICAO. Request For Information (RFI) 2007/2008. Technical report, Technical Advisory Group on Machine Readable Travel Documents, Canada, March 2007.
[16] ISO/IEC 14443. Proximity cards (PICCs). http://www.iso.org.
[17] A. Juels, D. Molnar, and D. Wagner. Security and Privacy Issues in E-Passports. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Greece, 2005.
[18] G. Kc and P. Karger. Preventing Attacks on Machine Readable Travel Documents (MRTDs). Technical report, IBM Research Division, NY, USA, 2006.
[19] A. Laurie. RFIDIOt. http://www.rfidiot.org/, May 2007.
[20] M. Lehtonen, F. Michahelles, T. Staake, and E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. In *Int. Conf. on Ambient Intelligence Development – Amid'06*, 2006.
[21] J. Monnerat, S. Vaudenay, and M. Vuagnoux. About Machine-Readable Travel Documents: Privacy Enhacement Using (Weakly) Non-Transferable Data Authentication. In *Int. Conf. on RFID Security 2007*, RFID Security, July 2007.
[22] D. Ortiz-Yepes. ePassports: Authentication and Access Control Mechanisms. Technical report, Technische Univ. Eindhoven TU/e, Netherland, June 2007.
[23] H. Robroch. ePassport Privacy Attack. `http://www.riscure.com`, 2006.
[24] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC), Version 1.00. Technical report, Bundesamt für Sicherheit in der Informationstechnik, Germany, 2006.
[25] S. Vaudenay and M. Vuagnoux. About Machine-Readable Travel Documents. *Journal of Physics Conference Series*, 77, July 2007.
[26] B. Wing. e-Passport/MRTD Observations. Second Symposium on ICAO-Standard MRTDs, Biometrics and Security.
[27] M. Witteman. Attacks on Digital Passports. Riscure, July 2005.