access control, biometrics,
electronic passport,
privacy, skimming, tracking

Zdeněk ŘÍHA[1], Vashek MATYÁŠ[1]

PRIVACY ISSUES OF ELECTRONIC PASSPORTS

Electronic passports combine classical passport booklets with the smartcard technology, biometrics and cryptography. The communication with the electronic passports is based on contactless ISO 14443 technology, designed for the communication distance of 0-10 cm. This paper is focused on the privacy aspects of the electronic passports. Weaknesses of the basic access control and extended access control are discussed. Significant emphasis is put on passport fingerprinting which may allow guessing the issuing country. Aspects of biometric data formats, skimming, eavesdropping and active authentication challenge semantics are also covered. The conclusions sum up recommendations for passport holders and issuers.

1. INTRODUCTION

Electronic ID documents have the potential to make the binding of the document and the traveller more secure and to speed up the process of passing through the passport control. The ICAO (International Civil Aviation Organization – a UN organization responsible for civil aviation and international travel) has standardized the storage of some passport data in two machine processible lines already in the 1980s. As the amount of data stored in this Machine Readable Zone (MRZ) is very small (88 characters) and the only "security" factor is the check digit, new ways of storing data for automated processing were investigated. The 6th version of the Part 1 of the ICAO Document 9303 describing travel documents has introduced the technology of contactless smartcards, biometrics and symmetric and asymmetric cryptography into the passport world. The enhanced passport that is equipped with a chip and an antenna (allowing contactless communication) is called an electronic passport.

The introduction of the new technology into passports brought a lot of controversy including discussions about economic, political and privacy aspects of the new technology; see e.g. (FIDIS, 2006). This paper is focusing on the privacy issues related to electronic passports. At first the paper summarizes the technological aspects of the electronic passports including short description of Singapore and European extended access control. Next the paper focuses on a number of privacy issues including skimming, eavesdropping, passport fingerprinting, biometric formats and weak points of basic access control and extended access control.

2. THE TECHNOLOGY

The passport chip is compliant to the ISO 14443 standard (both variants – A and B – are allowed) that is designed to communicate over distance of 0-10 cm and supports also relatively complex cryptographic operations. Higher communication layer is based on the classical smart card protocol ISO 7816-4. The reading systems send so called APDU (Application Protocol Data Unit) commands and the chip responds with R-APDUs (response APDU).

[1] Faculty of Informatics, Masaryk University, Brno, Czech Republic.

Fig. 1. Chip and antenna integrated in the polycarbonate data page.

Fig. 2. In UK passports the chip and antenna are directly visible.

Up to 16 data files named as DG1 to DG16 (DG for Data Group) can store data in passports. DG1 contains the data from the MRZ (i.e., issuing state, first name, surname, passport number, nationality, gender, birth date, expiry date, and optional data – for example a personal number), DG2 contains the photo of the passport holder. DG3 is dedicated for fingerprints (images or templates; in EU images compressed by the WSQ algorithm must be used), DG4 may contain iris image. Remaining data groups contain information about the holder, issuing institution or the passport itself. DG14 and DG15 can contain cryptographic keys (see below).

2.1. PASSIVE AND ACTIVE AUTHENTICATION

Data integrity of the information stored in the chip is protected by a digital signature located in the EF.SOD file. The PKI (Public Key Infrastructure) hierarchy has a single level. Each country establishes its own CSCA (Country Signing CA), which certifies bodies responsible for issuing the passports (e.g., the state printers, embassies etc.). The signed data is a special structure containing hashes of all present data groups in the passport.

It is clear that a digital signature cannot prevent from making identical copies of the electronic passport content (including the EF.SOD file with the digital signature) – so-called cloning. Cloning attacks has been demonstrated (even using NFC enabled mobile phones) e.g. in (van Beek, 2009). Cloning of passports can be prevented by using a combination of cryptographic techniques and reasonable tamper resistance. In such a case a passport-specific asymmetric key pair is stored in the chip.

Whereas the public key is freely readable (stored in DG15 and its hash is digitally signed), the private key is not readable from the chip and its presence can be only verified using a challenge-response algorithm (based on ISO 9796-2) called the active authentication.

The point of the active authentication is to verify whether the chip in the passport is authentic. The inspection system (IS – a system that is able to retrieve information from the electronic passport and check/display/use the data) generates an 8-byte random challenge and asks the chip to authenticate. The chip generates its own random string and cryptographically hashes both parts together. The chip's random string and the hash of both parts are then signed by the chip's private key. The result is sent back to the inspection system, which verifies the digital signature.

2.2. BASIC ACCESS CONTROL

The contactless communication brings certain advantages over the contact communication (e.g. speed), but there are drawbacks as well. The most serious drawbacks are related to eavesdropping and to the ability to communicate with the chip without the consent of the passport holder. Indeed the simple version of the electronic passport (also called plain passport) does not protect the access to the data in any way. These passports can be read without any authentication; the communication is not encrypted and data can be eavesdropped.

Such passports brought a lot of criticism. One way to improve security is passport shielding located in the cover of the passport. In such cases communication is not possible while the passport is closed. Once the passport opens the shielding becomes ineffectual and the communication with the chip is possible. Shielding can help to stop unintended communication, but does not protect from eavesdropping when the passport is open and is being read. Unfortunately shielding makes also legitimate communication more difficult.

Another way to protect the data in electronic passports from unauthorized readings is the authentication of the IS, establishment of a session key and encryption of the communication. Such a protocol is called basic access control (BAC) and addresses the issue of the unintended reading as well as of the eavesdropping.

Because the basic data in the passport must be readable by border control staff of **any** country, it would be really difficult to implement secret (encryption or authentication) key management in a way that the border control staff (and other authorized parties) can read the data while nobody else can do. Therefore it was decided to implement the protocol in a way that will allow access to anybody who is able to read some data from the personal data page. Because the authentication requires the knowledge of certain information and such information can be only obtained after the passport is open, it is expected that passport will be read only by those who have the passport in their physical possession (i.e. this happens with the consent of the passport holder).

The passport key used during the basic access control is derived from the document number, the birth date of the holder and the passport expiration date. All these items are printed in the second line of the MRZ and are protected with a check digit (the OCR is error prone; hence the choice of data fields with check digits). These three entries are concatenated in an ASCII form (including their respective check digits) and are hashed using the SHA-1 function. The hash value is then used to derive two (112-bit 3DES) keys for encryption and MAC (Message Authentication Code). The challenge is obtained from the chip and then IS and the chip mutually authenticate. The session key is established and further communication is secured using Secure Messaging (in a mode providing both confidentiality and integrity of the data).

Efforts to include the optional data field of the MRZ in order to increase the entropy of the data used to derive the authentication key were rejected due to compatibility issues with existing implementations (SUPPLEMENT 9303, 2007). Due to weak security properties of the BAC the protocol will be replaced by a more secure Password Authenticated Connection Establishment (PACE) developed originally as a part of the Extended Access Control version 2 (EAC2, 2009) for the protection of German ID cards. The passports will use version 2 of the PACE protocol (while German ID cards use version 1). The PACE protocol might protect electronic passports already in 2014, but it will take years before the

support of BAC can be removed from newly issued passports for compatibility reasons. The access control of passports implementing PACEv2 is named Supplementary Access Control (SAC).

2.3. EXTENDED ACCESS CONTROL

While the general information stored in electronic passports (e.g. name, photo, digital signature) must be readable at any border, more sensitive biometric data in the form of fingerprints or iris images (also called secondary biometrics) should be protected with additional mechanisms referred to as the extended access control (EAC). ICAO Doc 9303 does not specify any details about the EAC. Currently there are two implementations of the EAC in the world: the Singapore one and the European one.

The Singapore EAC is protecting the fingerprints in the DG3 by a passport-specific 3DES symmetric key which must be used to authenticate the inspection system before reading the DG3 file. The inspection system does not need to know symmetric EAC keys of all passports; as the symmetric EAC key is stored in the passport in DG13 in the encrypted form. Each inspection system has an asymmetric key pair and the DG13 file contains the symmetric EAC key encrypted by the public key of **all** inspection systems authorized to access the secondary biometric data in the passport. DG13 therefore contains a sequence of the symmetric EAC key encrypted by the public keys of inspection systems. The protocol is straightforward, but is not able to cope with changes in the structure of inspection systems. Adding or revoking access of a particular inspection system to already issued passports is not possible.

European EAC is more flexible, but requires a heavy PKI infrastructure and more complex passport chips. The protocol was developed by the German Federal Office for Information Security (EAC, 2008). The European EAC is based on asymmetric cryptography and it is a combination of Terminal Authentication and Chip Authentication protocols.

The aim of the terminal authentication is to restrict reading of secondary biometric data to authorized inspection system. Each country establishes a CV (Country Verifying) certification authority that decides which other countries will have the access to sensitive biometric data in their passports. A certificate of this authority is stored in all passports issued by that country and it forms the starting trust point (root certificate) for the access control. Other countries wishing to access sensitive biometric data (in their own passports or in passports of other countries), must establish a DV (Document Verifier) certification authority. This authority will obtain the certificate from all countries willing to grant access to sensitive biometric data in passports they are issuing. The DVCA will then issue the certificates to end-point entities actually accessing the biometric data – the inspection systems.

During the terminal authentication the inspection system first sends the DV and IS certificates. After the passport verifies the certification chain it has to check whether the inspection system can access the corresponding private key. That is performed using a challenge-response protocol. If the authentication succeeds, the inspection system can access sensitive biometric data (i.e. read the DG3 and/or DG4 files).

As the computational power of electronic passports is limited, simplified certificates (card verifiable certificates) are used instead of common X.509 certificates. An interesting point is the verification of certificate validity. As the chip has no internal clock, the only available time-related information is the certificate issue date. If the chip successfully verifies the validity of a given certificate issued on a particular day, it knows that this date has already passed (or is today) and can update its own internal time estimate (if the value is newer than the one already stored).

In addition to the terminal authentication, the European EAC also introduces the chip authentication protocol, which eliminates the low entropy of the BAC key and also may replace active authentication, as the access to the private key in the chip is verified (the public key is stored in DG14 and its integrity is checked during the passive authentication).

An inspection system reads the public part of the Diffie-Hellman (DH) key pair from the passport together with the domain parameters (stored in DG14). Then the inspection system generates its own ephemeral DH key pair (valid only for a single session) using the same domain parameters and sends it to the chip. The chip as well as the inspection system can then derive the shared secret based on available information. This secret is used to construct two session keys (one for encryption and the other one for MAC) that will secure the subsequent communication by Secure Messaging.

3. SKIMMING

3.1. CONTACTLESS COMMUNICATION

The communication with electronic passports is contactless and is based on the ISO 14443 standard with the nominal communication distance of 0-10 cm. However, with a more powerful reader it is possible to achieve longer communication distances. (Kfir & Wool, 2005) discusses the aspects of communication with the chip over a distance longer than the nominal 10 cm and concludes that the distance of 40-50 cm is achievable with commonly available technology. (Kirchenbaum & Wool, 2006) presented a working solution able to communicate over the distance of 25 cm confirming the theoretical findings presented in (Kfir & Wool, 2005). The German Federal Office for Information Security performed a set of experiments with similar results (Kügler & Naumann, 2007; MARS, 2008). Their study concludes that active communication with the chip is possible from the distance of 15-25 cm.

Passive eavesdropping does not have to power the chip; the aim of the eavesdropping is to monitor an existing communication. The eavesdropping distance can be different for the forward communication (reader to chip) and backward communication (chip to reader) and different for type A chips and type B chips. In general the eavesdropping distances are much longer than distances for which active communication with the chip is achievable and for type A chips the forward communication can be eavesdropped from longer distance than the backwards communication (Hancke, 2008). (Robroch, 2006) mentions eavesdropping distance of 25 m for forward communication and 5 m for backward communication without specifying more details. (Finke & Kelter, 2004) presents results for the eavesdropping distance of 2-3 meters. (MARS, 2008) discusses the theoretical aspects of eavesdropping of the communication and describes eavesdropping experiments for the distances up to 2.6 m.

In addition to the published papers there are also numerous rumours claiming that eavesdropping of both the directions is possible from tens or even hundreds of meters with a directional antenna.

3.2. DETECTING THE PRESENCE OF ELECTRONIC PASSPORT CHIPS

Active communication with the chip allows detection of electronic passports within the reach of the inspection system. When searching for the available chips the reader performs so called polling (described in ISO 14443-3), alternating REQA and REQB commands to locate type A and type B chips. In certain situations it may be sufficient for an attacker to know there is any chip in the reader's reach, in certain situations a nationality is what the attacker needs to know (e.g. the idea of a bomb triggers by an electronic passports of a holder of a particular nationality (Mahaffey &Hering, 2006)), in other case a particular passport is the subject of interest.

An electronic passport chip can be relatively easily differentiated from other ISO 14443 chips in most cases. This is a feature intended for the inspection systems to quickly focus on electronic passport chips in environments were many chips are within the reach of the reader (e.g. electronic visas). The method to identify electronic passport chips is the Application Family Identifier (AFI). The hexadecimal value of 'E1' has been allocated for electronic passports. The AFI is a part of the historical bytes of the ATS for type A chips. For type B chips the AFI is already a part of the command REQB('E1') requesting response only from electronic passports of type B.

3.3. CHIP IDENTIFIERS

Before the reader can communicate with the chip of the electronic passport it must choose one of the chips available to communicate with. This part of the protocol is called the anticollision and each chip needs a "unique" identifier. The anticollision algorithm is different for type A and B of the chips. For the type B of the chips the identifier (called PUPI – Pseudo-Unique PICC Identifier) is generated

(pseudo)randomly by the chip each time the chip is powered up by the reader[2]. The type B chip identifier is 4 bytes long and anticollision for type B chips is based on timeslots. Type A chips have identifiers of the length of 4, 7 or 10 bytes where the first byte codes the type of the identifier. Type A identifiers can be fixed for the whole lifetime of the chip or can be random. Fixed chip identifiers allow easy tracking of the passport.

ICAO does not make type A or B chips more favourable, but it recommends using random chip identifiers for increased privacy. Indeed most countries use random chip identifiers in their passports (type A chips with random identifiers or type B chips). One of the few exceptions is Italy using double size fixed chip identifiers in their type A chips.

A malicious country wishing to track their citizens might modify the randomness of the random chip identifiers. Using a single "random" value per passport would be too apparent, but using a set of alternating values per passport or using a more complicated algorithm (e.g. encrypting an ID of the passport concatenated with a few random bits by a secret key known only to the passport issuer) would be more difficult to reveal. As the first byte of the 4-byte long chip identifier must be '08' there are only 24 bits at the disposal. Such schemes (or worries) were described in theory, but there are no reports about being used in practice by any country.

3.4. BAC CHALLENGE

The only ICAO APDU commands used in BAC-protected passports before BAC authentication are SELECT ICAO AID and GET CHALLENGE. The challenge for BAC authentication is 8-byte long random number generated by the passport. The options for the passport to generate non-random challenges are basically the same as in the case of non-random chip identifier described above.

4. PASSPORT FINGERPRINTING

The aim of the access control in electronic passports (BAC, EAC) is to allow reading of data only after proper authentication of the inspection system. With the exception of plain (non-BAC protected) passports it is not possible to read the content of the chip without knowledge of the MRZ on the data page of the passport. Yet it is possible to communicate with a passport, e.g. to get the challenge (to authenticate). ePassport technology as defined by ICAO is based on open standards. There are many manufacturers in the world offering the ePassport technology. If a property of the passport is not directly prescribed by the standards then the manufacturers can choose how to implement the functionality. As a result different passports can behave in a bit different way and the difference might be recognizable even before the BAC authentication. Among others passport fingerprinting has been described by German and Dutch researchers (Richter et al, 2008).

There is no need for passport fingerprinting of plain passports, where the data can be read directly[3]. For example the early Belgium passports (issued before June 2006) do not implement BAC (Avoine et al., 2007). As Belgium passports store also the image of the holder's signature the danger of e.g. identity theft can be realistic. The passport data can also be read after a successful attack on the BAC (see below); in such situations the passport fingerprinting can be an initial step trying to guess the issuing country to speed up the BAC attack.

[2] The ISO14443-3 standard also allows the Pseudo-Unique PICC Identifiers to have fixed values (so called diversified fixed identifiers). Although such chips do exist probably no passport chips are based on such configurations.

[3] Although it may be technically easy, reading the content of the passport without the holder's consent may break the data protection rules and may not be legitimate (Kosta et al., 2007).

4.1. THE APPLICATION PROTOCOL

At the level of the application protocol the inspection system communicates with the passport by using APDUs according to ISO 7816-4. The ICAO 9303 standard prescribes only basic positive behaviour of the passport and ISO 7816-4 allows multiple status words.

Having 6 real passports of different countries labelled A, B, C, D, E and F we can try to find commands that will show different behaviour of different passports. The first command can be a reading command protected with Secure Messaging without the preceding authentication and session key establishment. All passports correctly reject the command, but the status word varies. Passport A responds with '68 00', passports B and C respond with '6E 00', passport D responds with '68 82', passport E responds '6A 88' and passport F responds with the status word '6A 82'.

Another example is based on selecting files. Passports protected with BAC must deny reading of files before the authentication is performed. But it is not specified whether also selecting the files should be rejected. Looking at the passport A-F we can see that passports A, B and C always reject selection of files with '69 82'. Passports D, E and F leak the existence of files. Selection of existing files succeeds (status word '90 00') while selection of non-existing files fails (status word '6A 82'). It can also be recognized that passport E contains DG11 and DG12 files.

Using multiple commands it is possible to distinguish more and more passports. For details and other commands see e.g. (Richter et al, 2008; Říha & Chareau, 2008). There is, however, no guarantee that a set of commands must exist to distinguish between two passports.

Recently it has been shown (Chothia & Smirnov, 2010) that certain French passports respond with different code to MAC errors and nonce errors during the initial mutual authentication. This allows tracking of a particular passport once a valid BAC session initialisation has been eavesdropped.

4.2. ANTICOLLISION AND TRANSPORT PROTOCOL TIMING, ERRORS AND OTHER FACTORS

On the lower level of the ISO 14443 communication we can look at discriminating factors such as type of the chip (A or B), length of the chip identifier, the ATR (Answer To Reset) or ATQB (Answer to Request, Type B). Another way how to distinguish different implementations of electronic passport chips is to measure the time the chip needs for certain operations. We cannot directly read data (in a BAC passport without authentication), but there are usable commands both at the APDU and ISO 14443 level. For example we can measure the time the chip needs to respond to the Request for Answer To Select (RATS) with its ATS.

Interesting distinguishing factors can be errors (deviations from standards). Some chips for example do not perfectly follow the state diagrams of the ISO 14443.

Passport fingerprinting can work well only if we are able to compare the passport fingerprint with a database of passports. If we do no know the behaviour of e.g. Japanese passport we logically cannot identify Japanese passports. This can be a limiting factor in practice, but building such a database can be trivial for e.g. a hotel receptionist.

5. OTHER ISSUES

5.1. CHALLENGE SEMANTICS

The fact that during the active authentication the passport chip digitally signs any challenge without knowing its possible semantics can be misused by inspection systems that can generate the challenges in a non-random way (EAC, 2008). The challenge may code e.g. the place and time of the passport inspection. In addition the challenge might also include the passport identifier and the above mentioned data could be digitally signed by the inspection system. To reduce the resulting size the data could be message-digested to fit the fixed size challenge length.

Having the digital signature of the chip over the challenge with given semantics is a strong argument that the passport chip was at a certain time at a certain place. The signature is transferable and third parties can verify the process of forming the challenge and check the digital signature. The need of the chip's private key for signing the challenge proves at least that the chip has seen the challenge. Having trust in the inspection system and knowing its public key and the algorithm of forming the challenge allows to proof the challenge was indeed generated by the inspection system at the given time and place. The challenge forming algorithm may also be combined with chained hashing of the previous border crossings so that it is not possible to modify the logs/challenges later. Because of the challenge semantics attack against the active authentication protocol some countries (e.g. Germany) decided not to implement the active authentication in their passports.

A similar signature-based challenge response protocol is used for authentication of the inspection system during the terminal authentication. In this case the challenge is generated by the chip and digitally signed by the inspection system. Although there should normally by no privacy issues with the inspection system, (Vaudenay & Vuagnoux, 2007) give an example of a malicious passport of a journalist passing the security control with a forged passport and threatening the border guard having the evidence in the form of the signed challenge with a particular semantics. Such an attack is however not realistic in practice, as the terminal authentication can be performed only after the chip authentication passes successfully and the journalist would need the private part of the chip DH key whose public part is stored in DG14 and as such protected by the passive authentication.

5.2. WEAKNESSES OF BASIC ACCESS CONTROL

BAC is based on a standard mutual authentication technique, which is considered to be secure as long as the keys are kept secret. In the case of electronic passports the keys are not secret in the classical sense as they are derivable from the data printed in the passport, but even so could prevent the random remote reading. This is, however, slightly problematic as the data used to derive the key do not necessarily have much of entropy. Although the theoretical maximum is 58 bits and in case of alphanumerical document numbers even 74 bits, real values are significantly lower. Let us discuss the particular entries in more details (Hoepman et al., 2006; Matyáš et al., 2008):

• Holder's birth date: one year has 365 or 366 days, theoretical maximum is 100 years, i.e., around 36524 days total (15.16 bits of entropy). If we know or can see the passport holder then his or her age can be realistically estimated with a precision of 10 years (3652 days, 11.83 bits entropy), often even more accurately.

• Day of expiry: the maximal validity of passports is 10 years (therefore approximately 3652 days, 11.83 bits entropy). Passports of children can have a shorter validity (typically 5 years).

• Document number: 9 characters are dedicated for the document number. Shorter document numbers must be padded with padding (<) characters and longer document numbers must be truncated. Document numbers consisting of digits only (and the padding character <) allow for the total number of 11^9 combinations (31.13 bits of entropy); if passport numbers can be alphanumerical then the maximum is 37^9 of combinations (thus 46.88 bits of entropy). These values can be accomplished only when the passport numbers are truly random. And that is often not the case. In many other countries the passport numbering is not random and the more you know about the passport numbering policy the less entropy the passport number bears. Many countries assign sequential numbers to their passports.

• Every entry is followed by the check digit. The algorithm is publicly known and the check digit does not introduce any new information.

To estimate the (total) entropy, we might sum the entropies of entries listed above. But that is correct only when the individual entries are independent. In typical setups a dependency between the document number and the expiration date will appear. Only for completely random document numbers and we can sum the entropies. Otherwise some dependency will be present and it is only the question of how much information about the numbering policy is known to the attacker. When an attacker has a significant knowledge, the total entropy can remarkably decrease. For example in the case of sequential document numbers and a country issuing 1 million passports uniformly over the year and in the case of a detailed knowledge of the document numbers issued on particular days the entropy of the document

number can decrease to about 12 bits. Total entropy then decreases from 58 respectively 74 bits to approximately 32 bits.

We can distinguish between two types of brute-force attack. Either the complete (successful) communication (of both the parties) is eavesdropped and then we try to decrypt it or we try to authenticate against the chip and then communicate with it to read the data. When eavesdropping the communication, we can store the encrypted data and then perform an off-line analysis. If the whole communication has been eavesdropped, we can eventually obtain all transmitted data. The disadvantage is the difficulty of eavesdropping of the communication (i.e., the communication must actually be in progress and we must be able to eavesdrop on it).

By exhaustive search of all probable combination of the fields from the MRZ we form the initial string that is hashed twice (for the detailed description of the protocol see e.g. (ICAO 9303, 2006)) to obtain the encryption key (the MAC key is not necessarily needed for this type of attack) and using the key we try to decrypt the data of the APDU. For each tested combination of fields we have to perform twice the SHA-1 hashing and once the 3DES decryption. An alternative attack can use the MAC key and MAC which requires two SHA-1 hashing, four DES encryption and one 3DES encryption, but can be used also in situations where only the commands from the reader has been eavesdropped (which is easier than eavesdropping on both directions). In such a case we have to come back to the passport to authenticate and read the data.

The derivation of a single key from the authentication data, data decryption and the comparison of the challenge takes around 1 microsecond on a common PC. The brute-force search of the space of authentication data with a size of 2^{32} thus can take around one hour. The practical demonstration of such an attack against Dutch passports has been published in (Witteman, 2005). His attack utilized an additional knowledge about the dependency between document number and the expiration date and the knowledge of the check digit within the document number reducing the total entropy to 35 bits.

An on-line attack against the chip can search the key space in the same way, but a single verification of the authentication data is significantly slower – we must communicate with the chip first and then we have to compute the MAC key and MAC code as well. A single on-line verification takes approximately 20 milliseconds for standard contactless readers and thus the attack is about 10 000x slower than an off-line attack.

It is necessary to realize that BAC does not restrict access to anybody who is able to read the MRZ. If you leave your passport at a hotel reception desk, BAC will not protect your data. BAC also cannot prevent so called one-bit attack, i.e. provided you know the MRZ of a particular passport and you only want to track the holder of that passport, the BAC will not be an obstacle to track or read the passport.

5.3. WEAKNESSES OF EXTENDED ACCESS CONTROL

The design of the Singapore EAC does not support revocation of inspection systems. Once the symmetric EAC key is encrypted with the public key of the particular inspection system and stored in the DG13 file there is no way to revoke the access of that inspection system to the fingerprint data. Therefore lost and stolen inspection system can present a risk to privacy of the secondary biometric data stored in electronic passports. The Singapore EAC also does not address well the international access to the fingerprint data (but this was not one of the design goals). Once a foreign inspection system is given access to fingerprint data there is no way to revoke the access (to fingerprint data in passports that have already been issued). If the inspection systems are online the system can be configured so that the inspection systems are turned into terminals not having access to the private key and only forwarding the encrypted symmetric keys to a secure online inspection system. This way the revocation can be implemented by revoking access of the terminal to the inspection system.

The European EAC also does not support revocation of the DV and IS certificates, but the certificates have only a very short validity (therefore we can talk about revocation based on expiration (Vaudenay & Vuagnoux, 2007)). The short validity of certificates helps to recover from situations when an inspection system is stolen or is compromised. Naturally only those passports that are often read with the advanced inspection procedure (i.e. certificates are sent, validated and the date estimate in the passport is updated) are protected from unauthorized reading by inspection systems with expired

certificates. This will be only the case of frequent travellers. Moreover it is not yet clear whether fingerprints will be read and matched each time the border is crossed. It is specifically required by the EAC specification that the date estimate is updated after the validation of the certificate chain (even without the following challenge-response authentication of the inspection system). As the certificates are not particularly sensitive this provision allows for kiosks not storing any private keys, but still being able to update the date estimate. Such kiosks can be located at airports or town halls. Indeed similar kiosks already exist and their primary function is to check the functionality of the chip in the passport.

The passport reading systems at the borders can also be connected to an online inspection system and work only in the terminal mode forwarding the challenge to the online inspection system (therefore the protocol is called **terminal** authentication).

The passive authentication in the form of the digital signature allows transferability of the data authenticity to third parties (Vaudenay & Vuagnoux, 2007). If a traditional passport is presented to a person, then the person will be able to see the age, name etc. But it will not be able to prove that information to a third party (unless makes a certified copy of the data page). In the case of electronic passports it is possible to copy the data group files together with the EF.SOD file and present the proof also to third parties. Non-transferable proof of signature knowledge would be more privacy protecting.

5.4. BIOMETRICS

The facial photo is stored in the DG2 file in the form of a JPEG/JPEG2000 bitmap image. There is no international standard for facial templates and the image must be viewable by the border guards as well therefore the facial biometrics must be stored as an image. Fingerprints on the other hand will typically not be visually checked by border guards and there are several standards specifying fingerprint template formats. ICAO Document 9303 supports the storage of images as well as templates. The EU legislation mandates the storage of images for interoperability reasons. From the privacy point of view biometric images are regarded more privacy intensive than processed templates. Raw biometric measurements can reveal additional information such as (a disposition to) diseases. Biometric images in facial and fingerprint based systems cannot be revoked (Kosta et al., 2007).

6. CONCLUSIONS

As a normal passport holder you cannot directly affect the design of your passport, the most important thing to protect your privacy is using the shielding sleeve and minimizing the physical access of others to your passport (e.g. at hotels).

Shielding can protect the electronic passport from unintended communication. Attackers cannot detect the presence of shielded electronic passports and cannot communicate with passport while shielded. The shielding can have the form of a Faraday cage using aluminium foil directly in the passport cover. For example passports of the USA use shielding integrated in the passport cover. If your country does not use shielding in the passport cover, you can still get a shielding sleeve working on the same principle e.g. (RFID shield, 2009). Another approach can be to insert a special “bookmark” into the electronic passport to block the communication. The bookmark attenuates electromagnetic field to a level that prevents the activation of the chip. Such bookmarks are available at e.g. (Priva’C, 2009).

Destroying the chip in the microwave oven or using a less powerful device (e.g. (MiniMe & Mahajivana, 2005)) eliminates the potential issues of the contactless communication, but exposes the traveller to a more thorough control at the border and cannot be recommended.

The issuing institutions can increase the privacy of passport holders by providing them with shielding sleeve together with the passports. The basic access control is the first step protecting the holder’s privacy (it is mandatory in EU) and the random the document number makes the BAC more efficient. Germany changed their passport numbering scheme in November 2007 to increase the entropy of the document number (Wikipedia, 2009). As soon as the standards will allow the move to PACE (the new protocol establishing Secure Messaging with strong encryption key even when the authentication data is short) the issuers should take the advantage of its security strengths.

The less data stored in the chip the better from the privacy point of view. The protection of secondary biometric data with an advanced access control mechanisms giving access only to authorized parties is a must. In the EU the storage of images of 2 index fingers is mandatory now; the access must be protected by the European EAC. In addition to strong protection of the private keys of the inspection systems and short validity of the DV and IS certificates there should be kiosks widely available for update of the time estimate for less frequently travelling passport holders.

The active authentication requires balancing the privacy with the document security. The active authentication protocol is an important security feature protecting passports from cloning attacks. Although the challenge semantics attack has been described and although an alternative protocol exists as a part of the EAC (the chip authentication protocol), the active authentication still remains the only protocol specified by the ICAO to check for the document authenticity.

BIBLIOGRAPHY

[1] AVOINE G., KALACH K., QUISQUATER J.J. Belgian Biometric Passport does not get a pass..., 2007, http://www.dice.ucl.ac.be/crypto/passport/index.html.

[2] van BEEK J., ePassports reloaded goes mobile, BlackHat Europe 2009, Amsterdam.

[3] Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Ver. 1.11, TR-03110, BSI, 2008.

[4] Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Ver. 2.02, TR-03110, BSI, 2009.

[5] Budapest Declaration on Machine Readable Travel Documents, FIDIS, 2006.

[6] FINKE T., KELTER H., Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, 2004.

[7] HANCKE G.P., Eavesdropping Attacks on High-Frequency RFID Tokens, Proceedings of the 4th Workshop on RFID Security (RFIDsec'08), July 2008, pp. 100–113.

[8] HLAVÁČ M, ROSA T., A Note on the Relay Attacks on e-passports? The Case of Czech e-passports, Tech. report 2007/244, Int'l Assoc. for Cryptologic Research, 2007.

[9] HOEPMAN J.H., HUBBERS E., JACOBS B., OOSTDIJK M., SCHREUR R.W., Crossing Borders: Security and Privacy Issues of the European e-Passport, in Advances in Information and Computer Security, Vol. 4266, LNCS, Springer Berlin, Heidelberg, 2006, pp. 152-167.

[10] CHOTHIA T., SMIRNOV V., A Traceability Attack Against e-Passports, 14th International Conference on Financial Cryptography and Data Security 2010, LNCS, Springer, 2010.

[11] ICAO, Document 9303, Edition 6, Part 1.

[12] ICAO, Machine readable travel documents (MRTDs): history, interoperability, and implementation, Release 1. September 2006.

[13] JUELS A., MOLNAR D., WAGNER D., Security and Privacy Issues in E-passports, Proc. of the First Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05), Washington, 2005, IEEE, pp. 74-88.

[14] KASPER T., CURLUCCIO D., PAAR C., An Embedded System for Practical Security Analysis of Contactless Smartcards, WISTP 07, May 2007.

[15] KFIR Z., WOOL A., Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), 2005, pp. 47-58.

[16] KIRSCHENBAUM I., WOOL A., How to Build a Low-Cost, Extended-Range RFID Skimmer, Cryptology ePrint Archive: Report 2006/054, 2006.

[17] KOSTA E., MEINTS M., HANSEN M., GASSON M., An analysis of security and privacy issues relating to RFID enabled ePassports, in IFIPSEC07, International Federation for Information Processing, Vol. 232, New approaches for Security, Privacy and Trust in Complex Environments, May 2007, pp. 467-72.

[18] KÜGLER D., NAUMANN I., Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen, Datenschutz und Datensicherheit, March 2007 (in German).

[19] MAHAFFEY K., HERING J., United States e-Passport Shield Failure Vulnerability, Blackhat 2006.

[20] BSI, Messung der Abstrahleigenschaften von RFID-Systemen (MARS), Projektdokument 1: Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation, 2008.

[21] MATYÁŠ V., ŘÍHA Z., ŠVENDA P., Security of Electronic Passports, UPENET, UPGRADE European NETwork, Upgrade Vol. VIII, No. 6, Dec. 2007.
[22] Minime (pseudonym), Mahajivana (pseudonym), RFID-Zapper, http://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN).
[23] ICAO TAG-MRTD/17 – WP11, Extended Access Control, Working paper for the 17th meeting in Montreal, NTWG, March 2007.
[24] Priva'C, http://www.ask.fr/uk/products_and_services/priva_c.html, accessed on July 2nd, 2009.
[25] RFID shield, http://www.rfid-shield.com/, accessed on June 1st, 2009.
[26] RICHTER H., MOSTOWSKI W., POLL E., Fingerprinting Passports, NLUUG 2008 Spring Conference on Security, 2008, pp. 21-30.
[27] ROBROCH H., ePassport Privacy Attack, Cards Asia Singapore, April 26, 2006.
[28] ŘÍHA Z., CHAREAU. J.M., Bezpečnost elektronických pas,. Mikulášská kryptobesídka 2008, Praha, December 2008.
[29] ISO/IEC JTC1 SC17 WG3, Supplement to Doc 9303, Release 6, September 21, 2007.
[30] VAUDENAY S., VUAGNOUX M., About Machine-Readable Travel Documents, Anti-counterfeit Image Analysis Methods, A Special Session of ICSXII, Journal of Physics, Conference Series 77, IOP Publishing, 2007, 012006.
[31] German entry for 'Reisepass', http://de.wikipedia.org/wiki/Reisepass.
[32] BRANDFORD W., e-Passport/MRTD Observations, 2nd Symposium on ICAO-Standard MRTDs, Biometrics and Security, Montreal, 2006.
[33] WITTEMAN, M. Attacks on Digital Passports, WhatTheHack Conference, July 2005, http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf.