An Overview of Electronic Passport Security Features

Zdeněk Říha

Faculty of Informatics, Masaryk University, Botanická 68A, 602 00 Brno, Czech Republic
zriha@fi.muni.cz

Abstract. Electronic passports include contactless chip which stores personal data of the passport holder, information about the passport and the issuing institution. In its simplest form an electronic passport contains just a collection of read-only files, more advanced variants can include sophisticated cryptographic mechanisms protecting security of the document and / or privacy of the passport holder. This paper describes security features of electronic passports and discusses their efficiency.

Keywords: Electronic passport, basic access control, passive authentication, active authentication, extended access control.

1 Introduction

A passport is a government issued identification document proving that the holder is a citizen of a particular country; belongs under its protection and is authorized to enter foreign countries. Passports must be resistant to counterfeiting, but the time available for passing through passport control is only limited. Machine readable travel documents have the potential 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) already standardized the storage of some passport data in two machine processible lines already in the 1980s. This zone (Machine Readable Zone – MRZ) contains basic data about the passport and its holder (name, surname, date of birth, date of expiry etc.) and it is printed in a standardized font so that it is machine readable (by optical character recognition – OCR) and can be processed by computer systems.

As the amount of data stored in the MRZ is only 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 ICAO Document 9303 describing travel documents uses the technology of contactless smartcards, symmetric and asymmetric cryptography and biometrics. The new passports equipped with chips and antennas (allowing contactless communication) are called electronic passports.

Although the electronic part of the passport remains optional at the worldwide level, the USA have asked all its Visa Waiver Program partners to introduce electronic passports and the European Union agreed on mandatory introduction of electronic passports in EU member states (to be exact, this regulation is not mandatory for the UK and Ireland and three non-EU countries – Norway, Switzerland and Iceland – do participate).

V. Matyáš et al. (Eds.): The Future of Identity, IFIP AICT 298, pp. 151–159, 2009.

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

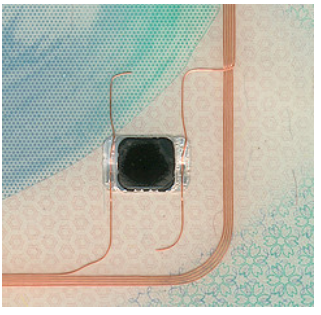

Fig. 2. Chip and antenna in UK passports

Table 1. Data groups which can be stored in electronic passports

Data group	Stored data
DG1	**Machine readable zone (MRZ)**
DG2	**Biometric data: face**
DG3	Biometric data: fingerprints
DG4	Biometric data: iris
DG5	Picture of the holder as printed in the passport
DG6	Reserved for future use
DG7	Signature of the holder as printed in the passport
DG8	Encoded security features – data features
DG9	Encoded security features – structure features
DG10	Encoded security features – substance features
DG11	Additional personal details (address, phone)
DG12	Additional document details (issue date, issued by)
DG13	Optional data (anything)
DG14	Data for securing secondary biometrics (EAC)
DG15	Active Authentication public key info
DG16	Next of kin

The chip and the antenna are integrated into the cover of the booklet or another page of the passport. The chip and antenna are typically not directly visible and can be only seen using a strong light (see Figure 1). An exception is the UK passport where the chip and antenna is laminated in one of the pages and can be directly seen (see Figure 2). An electronic passport can be easily recognized by the logo on the front page. The communication is contactless and complies with the ISO 14443 standard (both variants – A and B – are allowed). Technology based on ISO 14443 is designed to communicate over a distance of 0-10 cm and supports also relatively complex cryptographic chips and permanent memory of kilobytes or megabytes.

Higher communication layer is based on the classical smart card protocol ISO 7816-4 (i.e., commands like SELECT AID, SELECT FILE and READ BINARY are used).

The data in electronic passports are stored as elementary files in a single folder (dedicated file). Up to 16 data files named as DG1 to DG16 (DG for Data Group) can hold the data. See Table 1 for the overview of the content of the data groups.

Two additional files with metadata are also present. The file EF.COM contains a list of available data groups (and the information about versions used) and the file EF.SOD contains the digital signature of the data. The files EF.COM, EF.SOD, DG1 and DG2 are mandatory for all electronic passports. The data group DG3 will be mandatory in the EU countries after 28th June 2009 (and will be protected by an additional mechanism). All other data groups are optional.

2 Data Integrity (Passive Authentication)

Data integrity of the stored information is protected by a digital signature stored in the EF.SOD file. The file uses the SignedData structure of the CMS (Cryptographic Message Syntax) standard. The PKI hierarchy has a single level. Each country establishes its own CSCA (Country Signing Certification Authority[1]), which certifies bodies responsible for issuing the passports (e.g., the state printers, embassies etc.). These bodies are called Document Signers. Data in the passport are then signed by one of these Document Signers.

To verify signatures, the CSCA certificates of the issuing country must be available and their integrity must be guaranteed. Countries should use diplomatic exchange of the CSCA certificates, but experience shows that it is not simple in reality.

The certificate of the Document Signer is either directly stored in the passport (in the certificate part of the SignedData structure – and this is mandatory in the EU) or must be obtained from other sources (the issuing country, the ICAO public key directory –PKD, etc.). To verify whether a document signer's key was not revoked the CRL must be checked. CRLs must be regularly obtained from the ICAO PKD or by other means (some countries publish their CRLs on web or LDAP servers).

The data which is being signed is a special structure containing hashes of all present data groups in the passport. Integrity of each file can be verified separately (i.e., first the digital signature in EF.SOD is verified and then integrity of each file is checked by verifying its hash against the hash stored in the EF.SOD file).

It is not surprising that a digital signature alone cannot prevent identical copies from being made of the passport content (including the EF.SOD file with digital signature) – so-called cloning. As such, the inspection of the classical security features (security printing, watermarks, holograms, etc.) still makes sense, but the correspondence between the printed data and the data stored on the chip should also be verified.

3 Active Authentication (AA)

Cloning of passports can be prevented by using a combination of cryptographic techniques and reasonable tamper resistance. In such a case a passport-specific

[1] For more information on Public Key Infrastructure see for example the FIDIS document D3.2 http://www.fidis.net/resources/deliverables/hightechid/

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). This protocol is called the active authentication (AA) and it is an optional security feature of electronic passports Also for EU countries AA is an optional feature and indeed not all the countries implement it (e.g., Germany, Greece, Italy and France do not implement AA).

The aim of the active authentication is to verify whether the chip in the passport is authentic. The inspection system generates an 8-byte random challenge asks the chip to authenticate itself using it. 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. If the digital signature is correct the chip is considered to be authentic. The result of the AA only makes sense if the passive authentication has succeeded. Possible attacks might try to exploit weaknesses in the tamper resistance of the chip or can be based on the analysis of side-channels. If you have a genuine passport at your disposition you might also be able to produce a "copy" that talks back to the genuine passport when the active authentication needs to be performed. For a more detailed description of such a proxy (also called relay) attack see e.g. [2, 4].

There is an interesting privacy attack against an AA passport. If the challenge sent to the chip is not completely random, but rather specifically structured (for example encoding place and time), the inspection systems can store the challenge and the signature as a proof that the passport in question was at the given place at the given moment. In reality, such a proof would have to face the fact that the passport signs any arbitrary challenge at any place and the evidence value is therefore very limited. Even so some countries (e.g. Germany) decided not to implement the active authentication in their passports because of this privacy threat.

4 Basic Access Control (BAC)

Basic access control is a mechanism that prevents reading of the passport data before the authentication of the inspection system (i.e., prevents so-called skimming). The authentication keys are derived from data printed in the machine-readable zone of the data page. The document number, the birth date of the holder and the passport expiration date are used. All these items are printed in the second line of the machine readable zone and are protected with a check digit (the optical character recognition is error prone; hence the choice of data fields with check digits). During the authentication, session keys are established and further communication is secured using Secure Messaging, protecting the data transfer from eavesdropping.

BAC is based on a standard mutual authentication technique, which is considered 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 can prevent the random remote reading. Unfortunately the data used to derive the key do not necessarily have much 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 detail [3, 9]:

- 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). The holder's age can be realistically estimated with a precision of 10 years (3652 days, 11.83 bits entropy), often even more accurately.
- Day of expiry: 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 numbers can be alphanumerical then the maximum number is 379 of combinations (thus 46.88 bits of entropy). These values can be accomplished only when the passport number is truly random. And that is often not the case. Many countries assign sequential numbers to their passports. In such cases passport numbers and expiry date (and date of issue) are not independent.
- 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. Often the date of expiry and passport number is not independent. Then the total entropy does not reach the sum of individual items. 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. The brute-force key search can be then mounted against a significantly smaller number of possible keys [10].

Intended communication range of devices compliant with ISO 14443 is 0-10cm. This does not necessary mean that eavesdropping on longer ranges is not possible, but an attacker has to cope with a low signal-to-noise ratio problem. Whereas the signal from the inspection system (reader) is detectable at longer distances, eavesdropping of the data sent from the chip becomes more difficult with distance. For discussions about the possible ranges for skimming and eavesdropping see e.g. [5, 7]. The eavesdropped authentication data can be used to mount an off-line key search attack, where the low entropy of the static key can be used to reduce the key space for brute-forcing the key.

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 (Message Authentication Code) key and MAC code as well. A single verification then takes approximately 20 milliseconds for standard contactless readers and 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 machine readable zone. If you leave your passport at a hotel reception desk, BAC will not protect your data. On the other hand, there is no additional information

stored in chip than printed in the passport (in EU this is even a legal requirement; except for the fingerprints, of course).

There are also other issues related to contactless communication technology where BAC cannot help. First of all it is possible to remotely detect the presence of passive contactless chips. Second even before the BAC it is possible to communicate with the chip (e.g., to start the BAC). Anti-collision algorithms need unique chip IDs to address the chips. These chip IDs are typically randomly generated each time the chip is powered, but some chips of type A use fixed chip IDs, which makes their tracking very simple. Similarly some error codes may leak information about the chip manufacturer and/or model, which might also increase the chances of guessing the issuing state [8].

5 Extended Access Control (EAC)

EU passports will store fingerprints (in DG3) at the latest after 28th June 2009. Germany was the first European country storing fingerprints in their passports introducing their passports of the "second generation" already on 1st November 2007. Fingerprints in EU passports have to be stored as images in the WSQ format (lossy compression optimized for images of fingerprints). As fingerprints are considered to be more sensitive data than facial images (their recognition capabilities are much better), reading of DG3 will be protected by an additional mechanism. This mechanism is called the Extended Access Control and was developed by the German Federal Office for Information Security [1]. At the time of writing this paper (November 2008) EAC was not an international (ICAO) standard. The European EAC is based on asymmetric cryptography and is a combination of Terminal authentication and Chip Authentication protocols.

5.1 Terminal Authentication

The aim of the terminal authentication (TA) is to restrict reading of sensitive biometric data (fingerprints, possibly also iris images) to authorized persons, e.g. border guards. 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 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 (IS). See fig. 3.

Let's illustrate the process on an example. Each passport stores a CVCA certificate of the issuing country (e.g., Austria). If an inspection system (e.g., a Belgian one) needs to convince the passport that it is authorized to access sensitive biometric data, it must provide the DV certificate (the Belgian one in our case) signed by the issuing CVCA (Austria) and its own IS certificate (for that particular IS) signed by the DV

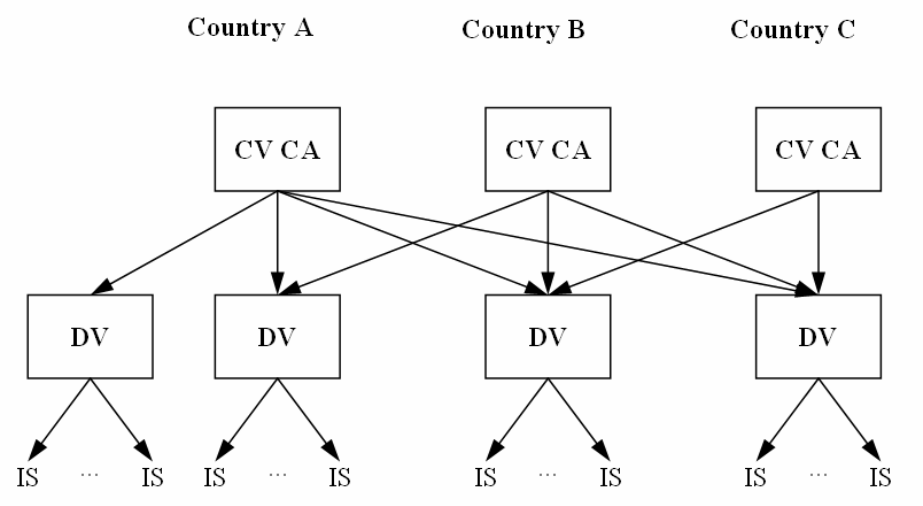

Fig. 3. A simplified view of an EAC PKI hierarchy

certification authority (i.e., Belgian in this case). After the passport verifies the whole 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).

The above mentioned process can be slightly more complicated as the CVCA certificates are updated from time to time (by link certificates) and the bridging link certificates have to be provided (and verified by the passport) at first.

Once the chain verification succeeds, the passport obtains the public key of the IS and its access rights. Only two access rights are specified at the moment, these are reading access to DG3 (fingerprints) and to DG4 (iris image).

As the computational power of electronic passports is limited, simplified certificates (card verifiable (CV) 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, then 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). It is clear that if a CVCA or DVCA issues (either by a mistake, intentionally or as a result of an attack) a certificate with the issue date in a distant future, the passport will then be rejecting valid certificates and will become practically unusable. For that reason, only the CVCA (link certificates), DV and domestic IS certificates are used to update the internal date estimate.

Short validity of certificates helps recovery 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.

5.2 Chip Authentication

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

An inspection system reads the public part of the Diffie-Hellman (DH) key pair from the passport (supported are the classic DH described in PKCS #3 standard and DH based on elliptic curves (ECDH) according to ISO 15946), 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 as the chip key and sends it to the chip. The chip as well as the IS 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. If the new session keys work well in the next command and reply, the chip authentication succeeded and the chip can be considered authentic.

Although chip authentication replaces active authentication, the chip can support both to allow verification of the chip authenticity at inspection systems that are not EAC-specific and only recognize international ICAO standards.

It is assumed that the protected biometric data will be initially accessible only among the EU member states. There have already been some speculations about involvement of countries like United States of America, Canada and Australia in the European extended access control system. Looking at the PKI structure of the EAC it becomes clear that is up to each member state to decide what other countries will have the access to data in the member state's passports.

6 Conclusions

The passive authentication securing authenticity of the data stored in electronic passports is a clear security benefit of the electronic part of the passport. But it can only be effective if the Country Signing CA certificates are available at all inspection systems (including relevant CRLs). How to achieve that in practice is still an open question.

While the BAC can prevent basic skimming, low entropy of the authentication key constitutes its major weakness. Efforts to include the optional data field from the machine-readable zone in the key computation (i.e., to increase the entropy) were rejected by ICAO in order not to break interoperability with existing systems. The only way to improve the strength of BAC is to use random alphanumeric document numbers. Some countries have already changed their numbering policy in order to make the attacks against BAC more difficult (e.g. Germany since Nov 2007 [11]). If you are worried that an attacker could communicate with your passport without your knowledge and either try to break the BAC or at least guess some information about the chip, just store your passport in a shielding cover which is widely available.

Active authentication preventing passport cloning is implemented by a surprisingly small number of countries. Cloning can also be prevented by chip authentication, which is a part of the EAC and will be implemented in the second generation EU

passport. EAC is also able to protect fingerprints and iris images stored in DG3/4 from unauthorized reading. The key management behind it is, however, not trivial – especially from the organizational point of view. And although the DV and IS certificates will have short validity to limit the use of stolen inspection systems, this will only be effective for passports of frequent travelers.

References

1. BSI: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110
2. 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), http://eprint.iacr.org/2007/244.pdf
3. Hoepman, J.-H., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R.W.: Crossing Borders: Security and Privacy Issues of the European e-Passport. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S.-i. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 152–167. Springer, Heidelberg (2006), http://www.cs.ru.nl/~jhh/publications/passport.pdf
4. ICAO, Document 9303, Edition 6 Part 1, Part 2 and Part 3
5. Kirschenbaum, I., Wool, A.: How to Build a Low-Cost, Extended-Range RFID Skimmer, http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html
6. Kosta, E., Meints, M., Hansen, M., Gasson, M.: An analysis of security and privacy issues relating to RFID enabled ePassports. In: IFIPSEC 2007 International Federation for Information Processing, May 2007. New approaches for Security, Privacy and Trust in Complex Environments, vol. 232, pp. 467–472 (2007)
7. Kügler, D., Naumann, I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen. Datenschutz und Datensicherheit (March 2007), http://www.bsi.de/fachthem/epass/dud_03_2007_kuegler_naumann.pdf
8. Richter, H., Mostowski, W., Poll, E.: Fingerprinting Passports. In: NLUUG 2008 Spring Conference on Security, pp. 21–30 (2008), http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf
9. Říha, Z.: Bezpečnost elektronických pasů, část I. Crypto-World 10/2006, http://www.crypto-world.info
10. Witteman, M.: Attacks on Digital Passports, WhatTheHack Conference, http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf
11. Wikipedia: German entry for 'Reisepass', http://de.wikipedia.org/wiki/Reisepass