Anatomy of Biometric Passports

Dominik Malě´ık and Martin Drahansk´y

Faculty of Information Technology, Brno University of Technology, Boˇzetěchova 2,
61266 Brno, Czech Republic
{imalcik,drahan}@fit.vutbr.cz
http://www.fit.vutbr.cz

Abstract. A recent trend in a field of personal identification documents is to use RFID *(Radio Frequency Identification)* technology and biometrics, especially (but not only) in passports. This paper provides an insight into the electronic passports (also called e-passport or ePassport) implementation chosen in the Czech Republic.
Such a summary is needed for further studies of biometric passports implementation security and biometric passports analysis. A separate description of the Czech solution is a prerequisite for a planned analysis, because of a uniqueness of each implementation[1].

Key words: passport, ePassport, electronic passport, biometric passport, RFID, chip, fingerprint, ICAO, algorithm, MRTD, Machine Readable Travel Documents

1 Introduction

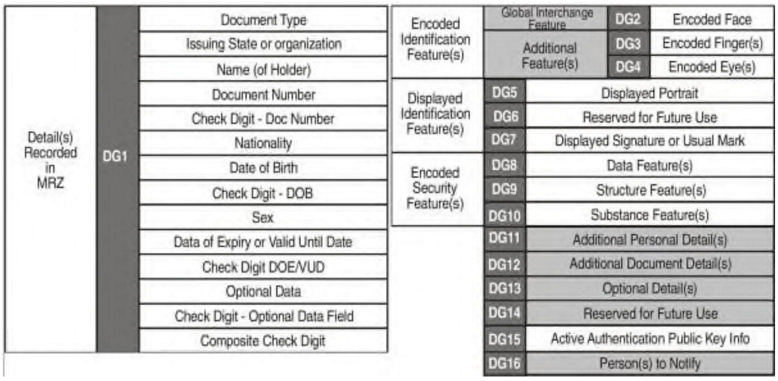
The idea of a better passport system incorporating biometrics has been alive for more than 20 years. However, it has taken considerable time to prepare all aspects for the new technology. Using biometrics to improve the system of travel documents is undoubtedly a crucial milestone. Naturally, there are security threats due to the fact that all biometric features are usually very sensitive information that has to be treated appropriately.

2 Passport chip

The RFID technology was chosen for implementation of the ePassports (all the electronic passports are labelled with an international logo – see the red circle in Fig. 2). The used chips have to meet standard compliant with ISO 14443 with modulation A or B – frequency for transmissions is 13,56 MHz with a short range (max. 15 cm) [7]. The passport RFID chip provides, among others, cryptographic functions, r/w memory modules accompanied with memory modules that are readable only for the tag itself (no information from these memory cells can be retrieved out of the device).

[1] Each country can choose the implementation details within a range specified by the ICAO *(International Civil Aviation Organisation – http: // www. icao. int/)*; moreover, specific security mechanisms are optional and can be omitted.

2.1 Passport chip memory



Detail(s) Recorded in MRZ	DG1	Document Type
		Issuing State or organization
		Name (of Holder)
		Document Number
		Check Digit - Doc Number
		Nationality
		Date of Birth
		Check Digit - DOB
		Sex
		Data of Expiry or Valid Until Date
		Check Digit DOE/VUD
		Optional Data
		Check Digit - Optional Data Field
		Composite Check Digit

Encoded Identification Feature(s)	Global Interchange Feature	DG2	Encoded Face
	Additional Feature(s)	DG3	Encoded Finger(s)
		DG4	Encoded Eye(s)
Displayed Identification Feature(s)	DG5	Displayed Portrait	
	DG6	Reserved for Future Use	
	DG7	Displayed Signature or Usual Mark	
Encoded Security Feature(s)	DG8	Data Feature(s)	
	DG9	Structure Feature(s)	
	DG10	Substance Feature(s)	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	Optional Detail(s)	
	DG14	Reserved for Future Use	
	DG15	Active Authentication Public Key Info	
	DG16	Person(s) to Notify	

Fig. 1. Memory data groups of passport RFID chip. Please notice especially the description of DG1-DG5 (source: [5]).

The memory is logically divided into two main regions - one is accessible from outside of the chip (via wireless communication), the second one provides a part of security by hiding its content – the hidden content is available only for internal functions of the chip.

The part of memory available for reading provides sixteen separated data groups (labelled as DG1, DG2, ..., DG16 – see Fig. 1). Each group incorporates different data. Dissimilar types of protection are used over the groups of the stored data. The data groups DG1, DG2, DG3 and DG5 are important within the scope of the biometric passports, because these groups are used for storing information related to identity check. [5]

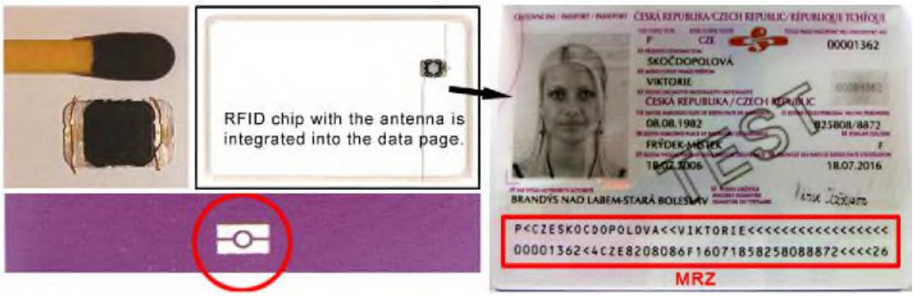

RFID chip with the antenna is integrated into the data page.
ČESKÁ REPUBLIKA/CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
P
CZE
00001362
SKOČDOPOLOVÁ
VIKTORIE
ČESKÁ REPUBLIKA / CZECH REPUBLIC
08.08.1982
825808/8872
FRÝDEK-MÍSTEK
F
18.07.2006
18.07.2016
BRANDÝS NAD LABEM-STARÁ BOLESLAV
TEST
P<CZESKOCDOPOLOVA<<VIKTORIE<<<<<<<<<<<<<<<<<<
00001362<4CZE8208086F1607185825808872<<<<26
MRZ

Fig. 2. On the top left: RFID chip without and with antenna; bottom left: the international logo of electronic passports; right: data page of a Czech specimen with labelled MRZ – Machine Readable Zone (source: [1]).

3 Use of biometrics

A proper biometric feature should be unique for each person and it should be invariable in time (usually from a specific age); given in the simplest possible way – it is an unambiguous identifier of a person. Moreover, some of the biometric features are well proven and have been even practically used for a long period of time – e.g. fingerprints in criminalistics. As it is not possible to give an exhaustive overview of biometrics, let us focus on the features that are important for contemporary passport implementation – 2D facial photo and fingerprints (the use of iris can be expected in the near future). [8]

3.1 Facial photograph

Facial photograph of an applicant is employed as a basic security element. This type of security is well known also from older types of documents. In classic paper documents, the facial photo primarily serves for visual identification by officers. Despite the officers' training and their ability to recognise a person even if there is some change in an applicant's appearance (moustache, haircut, glasses, etc.), the case of similar individuals (twins, siblings or even doubles) could lead to identity mismatch. If the facial photo is treated from a biometric point of view (not just as a picture of a person) – the face contains information that is invariant in time and can be measured, e.g. the distance between eyes, position of chin, position of nose, etc. These factors can affect the recognition process by providing additional information to the officer. Nonetheless, the twins will still look similar. That is why an absolutely different security component is needed (see chapter 3.2). [8]

Picture data storage The picture data (facial photo) is taken according to specifications in ISO19794-5 that defines conditions for acquiring this type of data: format, scene, picture properties, etc. The picture data is stored on the chip twice (DG2 and DG5 – see Fig. 1), both in JPEG/JPEG 2000 format.

The first occurrence is designated for laser engraving with following properties – grayscale, 60px distance between eyes, resolution of 620×796, stored in DG5. The second picture is encoded and stored in DG2 in full colour, resolution of 240×320 with max. size of 15 kilobytes. This smaller image is used for biometric identity check. [3], [5], [9]

3.2 Fingerprints

With respect to the facts introduced in chapter 3.1, the need for new reliable means of identity verification has been solved by introducing fingerprints. It has been proven that even fingerprints of monozygotic twins are significantly different. That means the two identities of twins can be obviously distinguished by matching the corresponding fingerprint with its stored digital representation (or with a paper record of the fingerprint). Even so, there still do exist possibilities for counterfeiting fingerprints. Nevertheless, the fraudsters have to face the problems with tricking the fingerprint scanners, because the scanners are being more often equipped with sophisticated liveness detection - especially when a security risk is expected. Sometimes it is simply almost impossible to cheat the fingerprint checking, because of a presence of an officer. Adopting this measure naturally does not result in an absolutely perfect protection against unwanted actions[2]. Nonetheless, the security level has rapidly increased with incorporating a fingerprint check. [8]

Fingerprint data storage Fingerprints are taken in compliance with ISO/IEC FCD 19794-4 and ANSI/NIST-ITL 1-2000 IS standards. The quality of stored fingerprint has to be marked with NFIQ (NIST Fingerprint Image Quality) equal to 3 or a better grade. In Fig. 1 can be seen that a DG3 has been designed to hold fingerprint data. Maximal data size of one fingerprint is 15 kB in compressed format WSQ specified in document IAFIS-0110 (V3), precisely according to the Gray-scale Fingerprint Image Compression Specification 1997. [9], [1]

4 The Czech implementation

The Czech electronic passport was introduced as a second device of this type in the EU. Since that time new types of security has been already introduced, however due to the backward compatibility of all solutions across the world and given minimal requirements of ICAO, the former threats will be still present. Other details regarding the whole Czech project (involved organisations, communication channels, passport producers, etc.) are not relevant for this paper[3].

4.1 Security

The main goal of the whole ePassport project is to preserve privacy of the personal data and prevent forgery of the travel documents. Different measures are used with respect to the importance of the particular aspect.

Mechanical and optical elements Security elements of this type are often used not only in passports (but also, e.g., bank notes, other types of personal documents, etc.). Although we do not aim at this type of security, let us mention at least some of them (not all of the listed bellow have to be necessarily employed in the last passport revision of the Czech Republic): serial numbers, fluorescent elements, relief stamping, engraving, guilloches, holograms, laser perforations, mechanic perforations, watermarks and many more.

[2] Absolute security does not exist.

[3] This information will be published in a different paper.

Basic Access Control (BAC) A very simple mechanism used for protection of information stored in DG1 and DG5 (see chapter 2.1). The BAC technique is based on two crucial principles – the first: data can be read only in case the passport is opened on the data page (if not, the RFID chip is shielded – a communication cannot be technically established); the second, the MRZ contains information which is used for the transmission password derivation). Actually, the data in DG1 and DG5 are the same as the information on the passport data page (see the right part of Fig. 2), that is why in the case the attacker has the ability to open the passport on the data page and read the MRZ, the information from the data page (and also from the DG1 and DG5) is not secret anymore.

The keys for the BAC are derived by SHA-1[4] from the MRZ, precisely from the passport serial number (9 characters), owner's date of birth (6 characters) and the date of expiry (6 characters). The result of the hash function is truncated to 16 bytes and divided into two parts (key A: 0th-7th byte; key B: 8th-15th byte) for 3DES. A key for the main communication is then established via 3DES encoded messages. [1], [2], [3], [7]

Active Authentication (AA) The active authentication serves as a protection against passport cloning. A couple of keys (private and public) is generated during the process of personalization of a new passport. The private key is stored in a part of memory that is inaccessible from outside of the chip (it is provided only in the hardware of the chip). The public key is freely available in DG15. [5]

The principle is then based on the asymmetric cryptography. Random data are generated and sent to a passport chip by a reader. The data are signed internally with the private key stored in the chip and sent back to the reader. In the last step, the reader verifies compatibility of the key pair and emits a result about authenticity of the private key. [3], [1]

Extended Access Control (EAC) The aforementioned BAC is definitely too weak to secure the sensitive biometric data – the fingerprints (DG3), in the future also the iris (DG4). Therefore, a new security specification was made. The EAC was specified in technical report BSI TR-03110 (Advanced Security Mechanism for Machine Readable Travel Documents – Extended Access Control). The EAC has been used in the Czech Republic since April 1, 2009 (it was brought to light together with incorporation of the fingerprints). [3], [1], [7]

Two cryptographic mechanism are being used within EAC:

Chip Authentication (CA, based on Diffie-Hellman) It is an alternative to Active Authentication (protection against chip cloning). In contrast to the Active Authentication, the CA does not suffer from so called challenge semantics. The challenge semantics can cause tracking of the owner's transfer in a specific case. That is why Germany did not include AA into their implementation of ePassport. After the DH process a cryptographically strong shared secret is available for encoding the following communication. [7]

[4] It is possible to use SHA-1 or SHA-2 (SHA224, SHA256, SHA384, SHA512).

Terminal Authentication (TA, based on PKI) Only approved terminals have permission to access the data groups with biometric data. The terminal has to be equipped with a valid certificate of particular country to access the data. Each terminal is set to a specific self destruction time period. The length of this period depends strictly on conditions of use of each terminal (from 1 shift to 1 month max.). Each terminal is labelled with unambiguous ID and can be blocked. [3], [1]

5 Conclusion

This summary of the ePassport implementation in the Czech Republic will be used as a basis for the next steps in an analysis of hardware (microscopic analysis, side channel analysis, etc.) and software (protocols analysis, firmware analysis, etc.) of such passports that will be performed within the next months.

6 Acknowledgment

This work is partially supported by the research plan ”*Security-Oriented Research in Information Technology*”, MSM0021630528 (CZ), by the grant ”*Advanced secured, reliable and adaptive IT*”, FIT-S-11-1 (CZ), by the grant ”*Information Technology in Biomedical Engineering*”, GD102/09/H083 and by the project ”*The IT4Innovations Centre of Excellence*”, ED1.1.00/02.0070.

References

1. Holenda, T.: Prezentace projektu ePas pro odbornou konferenci SystemováInte-grace *(Presentation of the project ePassport for conference System integration)*, presentation, Ministry of The Interior of the Czech Republic, 2009.
2. Holenda, T.: Odbornákonference Quality & Security *(Conference Quality& Security)*, presentation, Ministry of The Interior of the Czech Republic, 2007.
3. Mayer, P.: Biometricképasy v ˇCeskérepublice *(Biometric passports in the Czech Republic)*, presentation, Siemens ˇCR, 2007.
4. European Commission: Borders & Visas - Document security, Jan 2012. http://ec.europa.eu/home-affairs/doc\centre/borders/borders\doc\en.htm
5. The International Civil Aviation Organisation: Machine Readable Travel Documents (Part 1, Volume 2), ICAO, 2006, ISBN 92-9194-757-1.
6. Sheetal, S.: Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues, Viterbi School of Engineering, University of Southern California.
7. Raˇsek, L.: Elektronicképasy – jak funguj´ı *(Electronic passports – how it works)*, Viterbi School of Engineering, Czech Open System Users' Group, Conference proceedings, 2006.
8. Drahansk´y, M., Orság, F., Doleˇzel, M. et al.: Biometrie *(Biometrics)*, Brno, CZ, Computer Press, 2011, s. 294, ISBN 978-80-254-8979-6.
9. Maleë, F.: Druhágenerace elektronick´ych pasüa novágenerace elektronick´ych prükazüo povolen´ı k pobytu *(The second generation of electronic passports and a new generation of electronic documents)*, presentation, SmartCard Forum, 2010.