Hindawi Publishing Corporation
Journal of Biomedicine and Biotechnology
Volume 2012, Article ID 490362, 8 pages
doi:10.1155/2012/490362

Research Article

Anatomy of Biometric Passports

Dominik Malčík and Martin Drahanský

Faculty of Information Technology, Brno University of Technology, Božetěchova 2, 61266 Brno, Czech Republic

Correspondence should be addressed to Dominik Malčík, imalcik@fit.vutbr.cz

Received 25 May 2012; Accepted 18 July 2012

Academic Editor: Tai Hoon Kim

Travelling is becoming available for more and more people. Millions of people are on a way every day. That is why a better control over global human transfer and a more reliable identity check is desired. 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 the uniqueness of each implementation. (Each country can choose the implementation details within a range specified by the ICAO (International Civil Aviation Organisation); moreover, specific security mechanisms are optional and can be omitted).

1. Introduction

Nowadays it is still more necessary to be able to perform the identity check of passengers quickly and reliably—to prevent, for example, unauthorized border crossing, or to avoid any attempts of terrorist attacks, and so forth.

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 appropriately treated.

2. Motivation

After the incidents of the 11th September 2001 in New York, USA, a strong need for a better type of security at airports and borders all over the world was rising. This idea had existed before 11th September 2001. However, that particular terrorist attack can be considered as a strong impulse to start implementing a new security policy [1].

The reason for introducing the new security policy implementing electronic and biometric elements was not only an outcome of the terrorism. A better control over migration process with a lower number of illegal immigrants was also demanded. Another item on the list was an aggravation of the processes leading to faking documents. Last but not least, the target was to achieve a simpler, faster and a more accurate identity check process.

Use of technologies based on biometric features ensures almost all the aforementioned aspects. Security of storing and handling biometric information has to be treated in the best possible way, because this information can be easily misused.

3. Responsibility for the Global Passports' Evolution

A worldwide cooperation on unification of travel documents is under the auspices of the ICAO (http://www.icao.int/) *(International Civil Aviation Organisation)* with a mandate granted by the UN (http://www.un.org/) *(United Nations)* in 1947. With respect to the mandate of the UN, the ICAO issues recommendations and standards for employing new technologies in the field of travel documents (recently, the implementation of biometrics).

Figure 1: On the left: a Czech biometric passport specimen with circled international logo of electronic passports; top right: RFID chip without and with antenna; bottom right: data page with labelled MRZ (source: [1]).

The elements introduced by the ICAO, for example, unified passport data page or *Machine Readable Zone* (MRZ), can be seen in current versions of passports across the world. This can be, unquestionably, considered as a tangible result of the ICAO's work [1].

4. RFID Technology

Radio Frequency Identification is currently a widely used wireless identification technology. It is massively used simply for identification (chain supplement, personal identification cards, access cards, etc.), but its capabilities are much greater. It always depends on the type of the chip—some of them have only few bytes of ROM memory, but on the other hand, modern trend is to integrate various functions with sufficient amount of writeable memory. In the case of ePassports (all the electronic passports are labelled with an international logo—see the red circle in Figure 1) we can talk about cryptographic functions and 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).

RFID technology is based on two main devices—RFID tag (also known as the RFID transponder) and the RFID reader that has, in fact, usually also a writing ability, so the term "RFID reader" can be misleading. RFID tag can be either active or passive. The tag is commonly connected to an antenna. Active tags have onboard power supply (usually a battery) and active transmitter. Analogically to the active tags, the passive tags have no integrated power source and no active transmitter. The biggest difference between active and passive tags is the price and the operating range—passive tags' range is given in centimetres or tens of centimetres (ePassports incorporate passive RFID tags), in contrast to that, the active tags can communicate for up to kilometres [2].

All wireless technologies bring many advantages, but also disadvantages—in the scope of travel documents the biggest issue is security. It is clear that all wireless transfers can be eavesdropped or exposed to other known attacks—the manner of use of biometric passports can prevent some attacks like, for example, "man in the middle," because the reader is in close distance to the passport. That is why all communication transferring sensitive information has to be securely encoded.

For the ePassport RFID chips was chosen standard compliant with ISO 14443 with modulation A or B frequency for transmissions is 13,56 MHz with a short range (max. 15 cm) [19].

5. Passport Chip Memory

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 Figure 2). 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 the identity check [3].

Data Group 1. DG1 stores exactly the same information as those presented at the data page of the passport (see the bottom right part of Figure 1)—basic personal information

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 vaild 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 puplic key info	
	DG16	Person(s) to notify	

Figure 2: Memory data groups of passport RFID chip. Please notice especially the description of DG1–DG5 (source: [3]).

like name, date and place of birth, sex, date of expiration, and so forth.

Data Group 2. This data group is dedicated to a digital form of a facial photograph. Size limit is set to 15 kilobytes.

Data Group 3. The most recent security element of passports—fingerprint(s)—is stored in the DG5. Size limit is set to 15 kilobytes per fingerprint.

Data Group 4. Data group 4 should contain encoded iris data, but this feature has not been used yet.

Data Group 5. The last important data group (with respect to the biometrics) stores a photo of an owner that is depicted on the data page.

6. Introduction to Biometrics

Techniques based on biometric features are being widely deployed especially in the spheres, where a higher level of security or a precise identification is desired. However, all the technologies are becoming affordable for more ordinary purposes, as well. Therefore, we can expect a massive use of biometric-based products in the following decades.

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—for example, fingerprints in criminalistics. On the other hand, many of the biometric features have been explored relatively recently. 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) [4].

6.1. 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

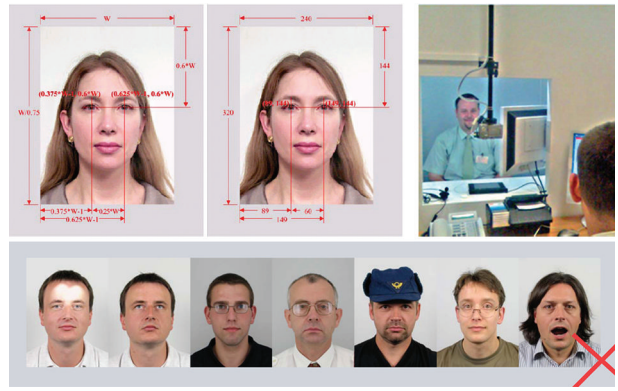

Figure 3: On the top left: an example of ideal facial photo with measures; top right: the Czech endpoint station from the officers' view; bottom: unacceptable facial photos (sources: [5, 6]).

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 (see Figure 3), for example, the distance between eyes, position of chin, position of nose, and so forth. 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 Section 6.2) [4].

Picture Data Storage. The picture data (facial photo) is taken according to specifications in ISO19794-5 that defines conditions for acquirement of this type of data: format, scene, picture properties, and so forth. The picture data is

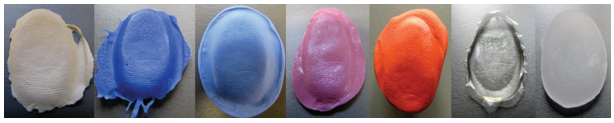

Figure 4: Examples of fingerprint fakes of different materials.

stored on the chip twice (DG2 and DG5—see Figure 2), 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, 6, 7].

6.2. Fingerprints. With respect to the facts introduced in the second paragraph of Section 6 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 undoubtedly distinguished by matching the corresponding fingerprint with its stored digital representation (of course, not only with the digital representation of the fingerprint, but also with, e.g, a paper record of that fingerprint—however, this variant is not dealt with in this paper). Even so, there still 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 (Absolute security does not exist). Nonetheless, the security level has rapidly increased with incorporating a fingerprint check [4].

Here might be considered that a potential attacker can use finger fakes to circumvent the fingerprint reader. Securing automated and unsupervised fingerprint recognition systems used for the access control is one of the most critical and most challenging tasks in real world scenarios. Basic threats for a fingerprint recognition system are repudiation, coercion, contamination, and circumvention [8]. A variety of methods can be used to get an unauthorized access to a system based on the automated fingerprint recognition. If we neglect attacks on the algorithm, data transport, and hardware (all these attacks demand good IT knowledge), one of the simplest possibilities is to produce an artificial fingerprint using soft silicon, gummy and plastic material, or similar substances [8–10]—see Figure 4. One example of the use of an artificial finger is shown in Figure 5, where you can see the fingerprint from a rubber stamp in comparison with the fingerprint from a real finger. For a really big amount of sensors, there is no difference between them, that is, the artificial fingerprint is processed and recognized as one concreter enrolled user from the database. To discourage

(a) (b)

Figure 5: Difference between a rubber stamp fingerprint (a) and a fingerprint from a real finger (b).

Figure 6: Examples of histopathological changes (upper row), skin discoloration (middle row) and a combination of both previous categories (lower row).

potential attackers from presenting a fake finger (i.e., an imitation of the fingertip and the papillary lines) or, even worse, to hurt a person to gain access, the system must be augmented by a liveness detection component [8, 11, 12]. To prevent false acceptance we have to recognize if the finger on the plate of the fingerprint sensor (also referred to as fingerprint scanner) is alive or not. There exist the following liveness detection methods [8]: perspiration, spectroscopic characteristics, ultrasonic technology, physical characteristics—temperature, hot and cold stimulus, pressure stimulus, electrical properties, bio-impedance, pulse, blood oxygenation, and some other not very reliable methods.

The second often neglected problem are skin diseases and their influence on fingerprint recognition [13–15]. These skin diseases (attacking fingers or generally hands) could be divided into three main groups [13, 14]: histopathological changes, skin discoloration, combination of histopathological changes and skin discoloration—see examples in the Figure 6. Histopathological changes mean that the structure of papillary lines is changed and the biometric system is not able to detect the separate papillary lines and valleys among them. Most of the sensors are based on physical principles, which do not allow acquiring of a fingerprint with a histopathological skin disease. The second group

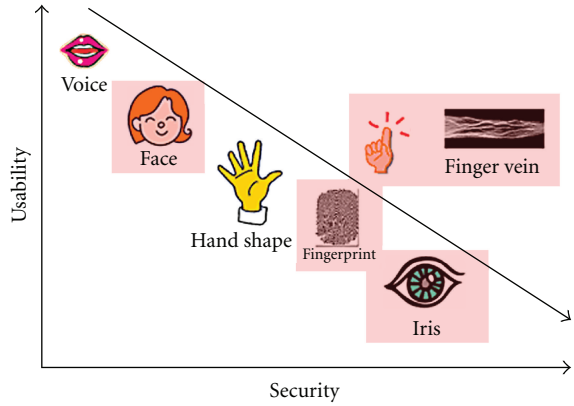

Figure 7: A simple comparison of biometric features with highlighted features proposed for future use in passports (source: [17]).

contains skin discoloration, that is, only the colour of the skin is changed, but the structure of papillary lines is kept unchanged. The most of sensors for fingerprint acquirement are not prone to this type of skin diseases. The last category combines both previous types. This category is very difficult for almost all of fingerprint sensors, because the combination of change of the structure of papillary lines and change of their colour is often resulting in a structure and colour, which is not recognizable as a fingerprint for further processing. In [13, 14], you can find not only more closer description of these skin disease categories including concrete disease examples, but basic information how you can evaluate the quality of a fingerprint, that is, recognize if the skin is affected by such a distortion, which does not allow to acquire and/or process the acquired fingerprint.

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 the stored fingerprint has to be marked with NFIQ *(NIST Fingerprint Image Quality)* equal to 3 or a better grade. In Figure 2 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 *(Wavelet Scalar Quantization)* specified in document IAFIS-0110 (V3), precisely according to the Gray-scale Fingerprint Image Compression Specification 1997 [1, 7].

6.3. Proposal for Further Use of Biometrics in Passports. With respect to the latest results in the sphere of biometrics, it is convenient to incorporate more biometric features into one device to ensure the quality of an automatic processing of personal identities and to prevent frauds in this area. Proposed features for a future use are primarily based on an iris recognition (use of the iris recognition has been already prepared in current passports, however the real application is still not common), veins of fingers recognition and especially combinations of these features with time-proven fingerprints (for a better illustration see Figure 7). A correctly implemented combination of aforementioned biometric features should be robust enough to provide all demanded properties of a passport system. Moreover, scanning of veins of a finger during a fingerprint scanning process should also provide liveness detection at the same time—that is a very important aspect in a fake fingerprint detection [8, 12, 16].

7. The Czech Implementation

The Czech electronic passport was introduced as a second device of this type in the EU (the passport system architecture can be seen in Figure 8). Since that time new types of security have been already introduced, however due to the backward compatibility of all solutions across the world and given minimal requirements of the ICAO, the former threats will be still present.

Despite particular rules were set by either the ICAO or consequently by the EU, there is still enough space for country-specific modifications. This results in a variety of solutions across the world that are different, but (mostly) compatible at the same time. The necessity for variability of local solutions rises from the fact that each country has its effective law and implemented related technologies that has to be incorporated into the passport employment.

7.1. Legislative Framework for Passports in the Czech Republic. A relevant legislative background for implementation of the mentioned security technologies was established by the European Union as a reaction to the 11th September 2001 terrorist attacks (This date is probably mentioned too often, however, consequence of this event was undoubtedly a very strong argument for employing a more sophisticated travel documents technology). To be more precise, a preparation of such a technology started much earlier, in 1981. The original proposals were set by the ICAO organisation and the EU regulations proceed from these recommendations.

Let us consider a coherent approach of the EU (2003) as a first important document for this paper. A brief sequence of milestones with respect to the Czech Republic implementation then came into being as follows [18].

20th June 2003. A coherent approach in biometrics implementation for biometric documents and data for the EU citizens, third country nationals and information systems.

13th December 2004. The council regulation No. 2252/2004 concerning standards for security features and biometrics in passports was issued by the Council of the European Union.

28th February 2005. The EU Commission Decision C(2005) 409 established the technical specifications on the standards for security features and biometrics in passports and travel documents.

15th June 2005. Government of the Czech Republic issues the ruling Nr. 740 that approves the process of implementation of the European Council regulations in the Czech Republic.

23rd December 2005. Signature of a contract with provider, STC, s.p. *(National Printer of valuables).*

1st September 2006. Launch of the first stage of the project—testing of the whole process with regular data.

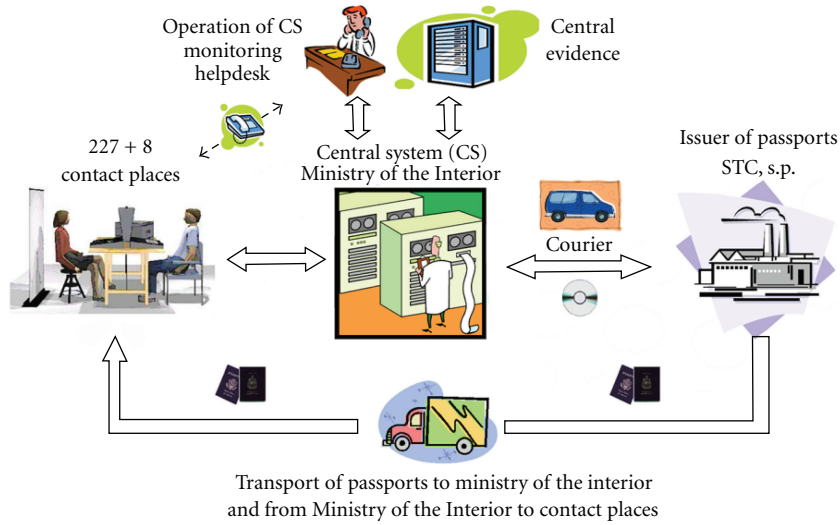

Figure 8: The Czech passport system architecture (source: Ministry of the Interior of the Czech Republic).

1st April 2009. Launch of the second stage of the project—implementation of fingerprints (as the second country in the EU, after Germany).

7.2. 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.

During the process of biometric passsport implementation (from assignment to the final product) several security aspects were treated, especially:

(i) A process security in general.

(ii) A security of involved buildings.

(iii) Mechanical and optical security elements.

(iv) Public key infrastructure (PKI).

(v) Fulfilment of international standards and recommendations.

(vi) Digital communication encryption.

(vii) Incorporation of biometrics.

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 items 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.

Basic Access Control (BAC). A very simple mechanism used for protection of information stored in DG1 and DG5 (see Section 5). 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 bottom part of Figure 1), 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 (It is possible to use SHA-1 or SHA-2 (SHA224, SHA256, SHA384, and SHA512)) 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 passports (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, 5, 6, 19].

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 [3].

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 [1, 6].

7.2.1. 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) [1, 6, 19].

Two cryptographic mechanisms 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 [19].

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 a 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 [1, 6].

7.3. Introducing of New Security Principles. Generally, it is always important to employ contemporary standards, for example, cryptographic standards, to ensure resistance to attacks against algorithms, protocols, hardware, and so forth. Use of new techniques is recommended also in the area of travel documents by the ICAO. Nevertheless, the introduction of technologies capable to handle such new versions of passports—with new algorithms and security principles—takes a certain time (in some countries less, in some countries more). However, till the time the old passport security mechanisms as, for example, BAC or manual identity check supported as regular principles, it will be possible to perform attacks against these poor mechanisms at least at places where the more secure mechanisms of current passports (fingerprints, iris) have not been implemented.

The best solution of this situation would be to prepare a completely new revision of passports with employing only contemporary secure mechanisms, but how to assure that all countries would be able to adopt new technologies necessary for handling the new passports? (And what about the compatibility with local law and regulations?). This is the biggest issue that cannot be easily solved, and so the backward compatibility will always open possibilities for attackers and fraudsters.

An absolutely different issue is the hardware design security. The hardware design of the Czech biometric passports has not been examined yet. That is why we cannot predict the current status of the hardware design now (of course there exist some general recommendations for designing secure hardware to prevent side channel attacks or microscopic analysis) (It is convenient to study these mechanisms especially from the area of smart cards where new countermeasures are usually introduced first).

A complete hardware analysis (including microscopic analysis, side channel analysis, etc.) is the aim of our future work—results and proposals for better implementation will be published in our future texts.

8. Conclusion

This paper sums up relevant details of the electronic passports implementation in the Czech Republic. This work 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 (in fact of the RFID chips) that will be performed within the next months.

Acknowledgments

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 European Regional Development Fund in the IT4Innovations Centre of Excellence project (CZ.1.05/1.1.00/02.0070).

References

[1] T. Holenda, *Prezentace Projektu ePas pro Odbornou Konferenci Systemová Integrace-Presentation of the Project ePassport for Conference System Integration, Presentation*, Ministry of The Interior of the Czech Republic, Holesovice, Czech Republic, 2009.

[2] S. She, "Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues," Viterbi School of Engineering, University of Southern California.

[3] The International Civil Aviation Organisation, *Machine Readable Travel Documents (Part 1, Volume 2)*, ICAO, Montreal, Canada, 2006.

[4] M. Drahanský, F. Orság, M. Doležel et al., *Biometrie (Biometrics)*, Computer Press, Brno, Czech Republic, 2011.

[5] T. Holenda, *Odborná konference Quality & Security-Conference Quality & Security, Presentation*, Ministry of The Interior of the Czech Republic, Holesovice, Czech Republic, 2007.

[6] P. Mayer, *Biometrické pasy v České republice-Biometric passports in the Czech Republic, presentation*, Siemens ČR, Praha, Czech Republic, 2007.

[7] F. Maleč, *Druhá Generace Elektronických Pasů a Nová Generace Elektronických průkazů o Povolený k Pobytu (The second generation of electronic passports and a new generation of electronic documents), Presentation*, SmartCard Forum, London, UK, 2010.

[8] M. Drahansky, *Liveness Detection in Biometrics, Book-Advanced Biometric Technologies*, InTech, Rijeka, Croatia, 2011.

[9] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial "Gummy" fingers on fingerprint systems," in *Proceedings of the Optical Security and Counterfeit Deterrence Techniques IV (SPIE '02)*, vol. 4677, pp. 275–289, usa, January 2002.

[10] B. Tan, A. Lewicke, and S. Schuckers, "Novel methods for fingerprint image analysis detect fake fingers," in *Proceedings of the Optical Security and Counterfeit Deterrence Techniques (SPIE '08)*, p. 3, 2008.

[11] M. Drahansky and D. Lodrova, "Liveness detection for biometric systems based on papillary lines," *International Journal of Security and Its Applications*, vol. 2, no. 4, pp. 29–37, 2008.

[12] M. Drahanský, *Fingerprint recognition technology: liveness detection, image quality and skin diseases [Habilitation thesis]*, BUT, Brno, Czech Republic, 2010.

[13] M. Drahansky, M. Doležel, J. Urbànek, E. Březinová, and T. Kim, "Influence of skin diseases on fingerprint recognition," *Journal of Biomedicine and Biotechnology*, vol. 2012, Article ID 626148, 14 pages, 2012.

[14] M. Drahansky, *Fingerprint Recognition Technology-Related Topics*, LAP, Saarbrcken, Germany, 2011.

[15] M. Drahanský, E. Březinová, F. Orság, and D. Lodrová, "Classification of skin diseases and their impact on fingerprint recognition," in *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, pp. 173–176, GI, Darmstadt, Germany, 2009.

[16] K. Dileep and R. Yeonseung, "A brief introduction of biometrics and fingerprint payment technology," *International Journal of Advanced Science and Technology*, vol. 4, pp. 25–38, 2009.

[17] Hitachi, Ltd.: About Finger Vein, http://www.hitachi-ics.co.jp/product/english/about_fv.htm.

[18] European Commission: Borders & Visas-Document security, http://ec.europa.eu/home-affairs/doc centre/borders/borders doc en.htm, 2012.

[19] L. Rasek, "Elektronické pasy-jak fungují (Electronic passports-how it works)," in *proceeding of the Czech Open System Usersf Group*, Viterbi School of Engineering, 2006.