Computer Modelling and New Technologies, 2009, Vol.13, No.3, 49–57
Transport and Telecommunication Institute, Lomonosova 1, LV-1019, Riga, Latvia

INTERNATIONAL STANDARDS FOR THE USE OF BIOMETRICS

G. Gromov

Transport and Telecommunication Institute
The Faculty of Management, Economics and Transport
The Department of Logistics
E-mail: gromov@tsi.lv

The systems of identification of an individual in the age of modern technologies are developing fast. However, not many of them received the global recognition. One of the world-wide accepted solutions is the use of such biometric features as the facial image and fingerprints of the person. Such globally interoperable biometric data shall be stored in the so-called "e-passport" and shall be readable in the countries other than the one, which has issued such passport.

This article raises the issues of the existing international technical and legal standards for production and use of e-passports containing the biometric data of individuals, necessary preconditions for the implementation of such standards at the national level, as well examines the regional approach of the European Union to this issue and the results, which were achieved to this day.

Keywords: *biometric features, security, e-passports, public key infrastructure, International Civil Aviation Organisation (ICAO) standards, European Union*

Part I

1. Introduction

The use of biometric features (referred further as biometrics) in the modern world has become increasingly extensive and multipurpose, both due to the rapid technical progress in this area and the growing security concerns.

It shall however always be remembered that actually took 40 years to develop the biometric technology into the one we know nowadays, as the work started as long time ago as back in 1968.

The use of biometrics as described in this article is presumed to increase the security of passports and other travel documents. But it has a spill-over effect on much broader range of subjects, such as:

- security of the states,
- control of legal migration,
- combating of illegal migration, people smuggling and trafficking in human beings,
- identity theft,

and many others.

The purpose of this article is to look on the current international standards, which are used in the area of biometrics, and, using as an example the European Union case, how and in which manner they are applied.

2. Regulations of European Union for the Usage of Biometrics

In order to properly examine the international standards in the area of biometrics, the close look on the practical value of biometrics is needed.

The experience of the European Union is an excellent example. Council Regulation 2252/2004/EC (entered into force on 18 January, 2005) has laid down standards for security features and biometrics in passports and travel documents issued by the Member States [1]. This Regulation applies to passports and travel documents issued by the Member States. It does not apply to identity cards issued by the Member States to their nationals or to temporary passports and travel documents having a validity of 12 months or less.

Additional technical specifications for passports and travel documents are established in accordance with the procedure referred to in Article 5(2) of this Council Regulation:

- additional security features and requirements including enhanced anti-forgery, counterfeiting and falsification standards;
- technical specifications for the storage medium of the biometric features and their security, including prevention of unauthorised access;
- requirements for quality and common standards for the facial image and the fingerprints.

As Council Regulation (EC) 2252/2004 has laid down standards for security features and biometrics in passports and travel documents, which are general and non-secret, the European Commission decided that they had to be completed with other technical specifications, which may remain secret. Following such a consideration and taking into account the procedure under Article 5(2) of the (EC) 2252/2004, on 28 February 2005 the Commission adopted Decision C(2005)409, establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by the Member States [2] (an authentic English version of the whole of specifications has not been established as the United Kingdom and Ireland did not take part in the adoption of this Decision).

The technical specifications mainly deal with the implementation of the integration of biometric features (facial image and fingerprints) on a secured storage medium in the passport. This adoption also triggered the deadline for the implementation of the facial image in the passport, which was August 28, 2006 at the latest.

On 26 June 2006, the European Commission adopted Decision C(2006)2909 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by The Member States, which supplements previous Decision C(2005)409 with new subsections 5.4., 5.5. and its subsections, 6.1., 6.2. and 6.3. The new subsections regulate the Public Key Infrastructure for Passports and Inspection Systems, Certificates, Standard Compliance, as well as Functional and Common Criteria Evaluation.

Taking into account the statement by ICAO as "recommendation" requirements and the role of ISO in adopting the standards on the basis of ICAO documents, it is necessary to follow both organizations' requirements to ensure compliance of the standards.

The Annex to the detailed EU requirements for e-passports mentioned in Commission Decision C(2006)2909 shall be considered as a consolidated version of international standards (both ICAO and ISO). No additional standards of only EU requirements are established under the scope of (EC) 2252/2004.

On 18 October 2007, a Proposal from the Commission was introduced for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by the Member States [3]. At the time of the Commission's proposal for Regulation (EC) 2252/2004 and the discussions on it in the European Parliament and the Council, no experiences with the use of biometric data for large-scale applications in travel documents were available. These new technologies of inserting chips with biometric data had not been applied or tried out before. During pilot projects of some Member States it appeared that the fingerprints of children under the age of six seemed not to be of a sufficient quality for one-to-one verification of identity. Furthermore, they are subject to important changes which make it difficult to check them during the entire period of validity of the passport.

Both for legal and security reasons it should not be left to the national legislation to define the exceptions from the obligation to provide fingerprints for passports and other travel documents issued by the Member States.

Consequently, the European Commission proposed an amendment to Regulation 2252/2004 in order to provide harmonised exceptions: children under the age of six years and persons, who are physically unable to give fingerprints, should be exempt from this requirement.

Furthermore, as a supplementary security measure and in order to provide additional protection for children, the principle of "one person – one passport" has to be introduced. It is also recommended by the International Civil Aviation Organisation (ICAO) and it ensures that the passport and the biometric features are only linked to the person holding the passport. It is more secure if every person has his/her own passport. If, for example, a passport is issued that also includes the person's children, indicating only the names and without photographs, only the biometric data of the respective parent would be introduced on the chip. The biometric information of the children would not be stored. As a consequence, the identity of the children cannot be checked in a reliable way. This could promoter child trafficking. It was postulated that introduction of the principle "One person-One passport" would help to avoid this negative effect.

During pilot projects in some EU Member States it appeared that the fingerprints of children under the age of 6 seemed not to be of a sufficient quality for one-to-one verification of identity. Furthermore, they are subject to significant changes which make it difficult to check them during the entire period of validity of the passport or travel document.

On May 28, 2009 the abovementioned proposal was finally adopted as the Regulation 444/2009 of the European Parliament and of the Council amending Council Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents issued by the Member States [4]. It was decided that children aged under 12 years are exempt from compulsory finger printing and not aged under

the 6 as it was mentioned in the Proposal. According to point 3 of Article 1 of the abovementioned Regulation additional technical specifications in accordance with international standards, including in particular the recommendations of the ICAO, for passports and travel documents relating to the following shall be established:

- additional security features and requirements, including enhanced anti-forgery, counterfeiting and falsification standards;
- technical specifications for the storage medium of the biometric features and their security, including prevention of unauthorised access;
- requirements for quality and common technical standards for the facial image and the fingerprints.

These provisions replaced the provisions under Article 2 of the Council Regulation (EC) 2252/2004.

The European Commission should also present the study until June, 2012 where reliability and technical feasibility, including through an evaluation of the accuracy of the systems in operation, of using the fingerprints of children under the age of 12 for identification and verification purposes should be examined.

As it is was previously mentioned EU requirements for biometrics in passports are based on the standards of ICAO, which were accepted by International Standards Organisation. Therefore there is a need to properly examine the interoperable global standards of biometrics, which were developed by the ICAO.

3. The International Civil Aviation Organisation and Its Impact on the Development of the International Standards

The first introduction of the interoperable global standard of biometrics in Machine Readable Travel Documents (MRTDs) was made public in 2003. Version 1.9 of Biometrics Deployment Technical Report discussed each of the issues in relation to the deployment of biometrics and was presented to the 14th ICAO Technical Advisory Group (TAG/MRTD) in mid-May 2003. TAG/MRTD endorsed the Technical Report, and ICAO subsequently adopted it as a key component of its global, harmonized blueprint for the integration of biometric identification information into passports and other MRTDs.

3.1. Doc. 9303

First published in 1980 as "A Passport with Machine Readable Capability", Doc 9303[5] is now published in three separate Parts [6].

Part 1 – Machine Readable Passport – Volume 1 Passports with Machine Readable Data Stored in Optical Character Recognition Format	Sixth Edition	2006
Part 1 – Machine Readable Passport – Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capabilities	Sixth Edition	2006
Part 2 – Machine Readable Visas	Third Edition	2005
Part 3 – Size 1 and Size 2 Machine Readable Official Travel Documents	Second Edition	2002

The Sixth Edition of Doc 9303 Part 1, in two volumes, was published in September 2006. Volume 1 sets forth the specifications for a Machine Readable Passport (MRP), characterized by a visual inspection zone and a machine readable zone (MRZ) containing essential identification and document details in optical character recognition (OCR)-B typeface. Volume 2 sets forth the specifications for biometric enhancement of the MRP to become an "e-Passport".

The third Edition of Doc 9303 Part 2 – Machine Readable Visas – was published in 2005. Specifications provide for a visa format in two sizes – Format A, sized to fill a passport page, and the smaller format B. Like the MRP, the machine readable visa is a standard format consisting of a visual inspection zone and a machine readable zone. However, the Third Edition requires that a space be provided for a portrait of the holder, and fewer layout options than the previous edition allowed.

The Second Edition of Doc 9303 of Part 3 – Size-1 and Size-2 Machine Readable Official Travel Documents, was published in 2003. Specifications provide for machine readable cards in two sizes: TD-1, an ID-1 size plastic card, and TD-2 having the dimensions defined for the ID-2 type card (ISO/IEC 7810). In addition to the visual inspection zone and the machine readable zone, the specifications provide for the addition of "optional capacity expansion technologies" to increase data storage on the documents.

3.2. Doc. 9303 Part 1

The current edition updates and replaces the specifications for MRPs as published in the fifth edition (2003) and represents a substantial modernization of the material contained in previous editions. In particular, this sixth edition incorporates the new globally interoperable standards for biometric identification of the holder and for the storage of the associated data on a contactless integrated circuit. In consequence, some other biometric identification methods and data storage media, described in the fifth edition, are no longer to be regarded as options within the globally interoperable standard.

The first volume, known as Doc 9303 Part 1 Volume 1, is an updated version of the fifth edition containing all the specifications required for a State to issue a MRP book where the State does not wish to incorporate the global facilitation for its citizens that will be available with machine assisted biometric identification.

It also defines the MRP specifications which allow compatibility and global interchange using both visual (eye readable) and machine readable means. The specifications lay down standards for passports which can, where issued by a State or organisation and accepted by a receiving State, be used for travel purposes.

The second volume, known as Doc 9303 Part 1 Volume 2, contains additional specifications for the globally interoperable system of biometric identification and its associated data storage utilizing a contactless integrated circuit. The specifications contained herein were drawn up following a detailed study over several years carried out by the ICAO Technical Advisory Group's New Technologies Working Group (NTWG) beginning in 1998. The study examined different biometric identification systems, concentrating on their relevance to the facilitation for a traveller in applying for and obtaining a biometrically enabled passport and in using that passport for travel between States.

The specifications for the new globally interoperable system contained in this Volume Two are only for use by States wishing to issue a passport designed to facilitate cross-border travel with enhanced security by incorporating the globally interoperable machine assisted biometric identification/data storage system. These States will therefore need to observe the specifications in both Volumes to conform to the standards laid down in ICAO Doc 9303 Part 1.

4. International Standards Organisation (ISO)

The technical specifications sections of Doc 9303, Parts 1, 2 and 3 have received the endorsement of the ISO. Due to cooperation between manufacturers of travel documents and equipment with TAG/MRTD on technical issues with the participation of ISO, the ICAO specifications have achieved, and are expected to continue to receive, the status of worldwide standards by means of a simplified procedure within ISO.

Taking into account the above-mentioned, Doc 9303 formally can be considered as international recommendations and not as standards.

5. E-Machine Readable Passports

According to ICAO, in implementing biometrics standards for MRPs, the key considerations are:

- Global Interoperability – the crucial need for specifying how the biometrics deployed are to be used in a universally interoperable manner;
- Uniformity – the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States;
- Technical Reliability – the need for provision of guidelines and parameters to ensure that Member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading the data encoded by other States can be sure that the data supplied to them is of sufficient quality and integrity to enable accurate verification at their end;

- Practicality – the need to ensure that recommended standards can be operationalized and implemented by States without having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards;
- Durability – the systems introduced will last the maximum ten-year life of a travel document, and future updates remain backwards compatible.
- Biometrics can be used to improve the quality of the background checking performed as part of the passport, visa or other travel document application process, and they can be used to increase the strength of the binding between the travel document and the person who holds it.

The major components of a biometric system are:

- Capture – acquisition of a raw biometric sample;
- Extract – conversion of the raw biometric sample data to an intermediate form;
- Create Template – conversion of the intermediate data into a template for storage;
- Compare – comparison with the information in a stored reference template.

These processes involve:

- the enrolment process which is the capture of a raw biometric sample. It is used for each new person (potential MRP holder), taking biometric samples to establish a new template. This capture process is the automatic acquisition of biometric features via a capture device such as a fingerprint scanner, photograph scanner, live-capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process – for example, standard pose facing the camera straight-on for a facial recognition capture; whether fingerprints are captured flat or rolled; eyes fully open for iris capture.
- the template creation process preserves the distinct and repeatable biometric features from the captured biometric sample and is generally via a proprietary software algorithm to extract a template from the captured image which defines that image in a way it can subsequently be compared with another captured image and a comparative score determined. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. Quality standards need to be as high as possible since all future checks are dependent on the quality of the originally captured image. If the quality is not acceptable, the capture process should be repeated.
- the identification process takes new samples and compares them to the saved templates of enrolled end users to determine whether the end user has enrolled in the system before, and if so, whether in the same identity.
- the verification process takes new samples of an e-Passport holder and compares them to the previously saved templates of that holder in order to determine whether the holder is presenting in the same identity.

In biometrics terminology:

- "verify" means to perform a one-to-one match between proffered biometric data obtained from the MRTD holder now, and a biometric template created when the holder enrolled in the system;
- "identify" means to perform a one-to-many search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

After a five-year investigation into the operational needs for a biometric identifier, which combines suitability for use in the MRP issuance procedure and in the various processes in cross-border travels, consistent with the privacy laws of various States, ICAO has decided that facial recognition shall become the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

As the result of such a study, ICAO Doc 9303 only considers three types of biometric identification (automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits). These are the physiological ones of:

- facial recognition (mandatory);
- fingerprint (optional);
- iris recognition (optional).

An international Standard, ISO/IEC 19794, composed of several Parts, provides specifications for these types of biometric identification. Issuing States shall conform to these specifications.

"E-Passports" is the term used by ICAO to simplify the understanding of globally-interoperable MRPs containing biometrics. The e-Passport has to be capable of being used by any suitably equipped receiving State to read from the document a greatly increased amount of data relating to the MRP itself

and to its holder. This includes mandatory globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems. The specifications require the globally interoperable biometric data to be stored in the form of high resolution images on a high capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. The specifications also permit the storage of a range of optional data at the discretion of the issuing State.

Any MRP that does not comply with the specifications given in ICAO Doc 9303 Part 1 Volume 2 may not be called an e-passport and may not display the e-passport logo.

The data storage capacity of the IC is specified to be a minimum of 32 kB, which is large enough to store the mandatory facial image and, also mandatory, a duplication of the Machine Readable Zone data. However, the optional storage of more than one facial image and/or fingerprint/iris images requires considerably larger data capacity. Some States are planning to use ICs with data capacities ranging from 64 kB to 1 MB.

The ICAO vision for the application of biometrics technology encompasses:

- specification of a primary interoperable form of biometrics technology for use at border control (verification, watch lists) as well as by carriers and document issuers and specification of agreed supplementary biometric technologies;
- specification of the biometrics technologies for use by document issuers (identification, verification and watch lists);
- capability of data retrieval for a maximum ten-year validity, as specified in Doc 9303;
- having a no proprietary element to ensure that any States investing in biometrics are protected against changing infrastructure or suppliers [7].

For this moment, specifications for MRTDs have been formulated and today almost 90 percent of the ICAO member states are issuing a MRP. Not only enabling the standardisation of document formats, MRTDs facilitate the accurate and efficient input of personal information to computerised systems serving border security and facilitation functions. The ICAO objective of having all the Member States issuing MRPs by April 1, 2010, is now very much attainable and not simply a target as it has been twenty years ago [8].

6. European Union Standards for Use of the Biometrics in E-Machine Readable Passports

As it was mentioned above, the Annex of Decision C (2006)2909 could be used as a guide for introducing the international standards of technical specifications for introducing e-MRPs.

The Annex is based on international standards, especially ISO standards and ICAO recommendations on Machine Readable Travel Documents, and accommodates:

- specifications for biometric identifiers: face and fingerprints;
- storage medium (chip);
- logical data structure on the chip;
- specifications for the security of the digitally stored data on the chip;
- RF compatibility with other electronic travel documents.

6.1. Face

The face as the primary biometric should have a standard compliance with the facial image and must be stored as Frontal image [9], according to:

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004;
- ISO/IEC 19794-5:2005, Biometric Data Interchange Formats – Part 5: Face Image Data.

The face is to be stored as a compressed image file, not as vendor specific template. Although both JPEG and JPEG2000 compression is standard compliant [10], JPEG2000 is recommended for EU-Passports because it results in smaller file sizes compared to JPEG compressed images. Storage requirements for JPEG compression are approx. 12–20 Kbyte per photo, but for JPEG2000 compression approx. 6–10 Kbyte per photo.

Photograph Taking Guidelines taking into account the requirements of facial recognition technology have to be adopted according to ICAO standards [11].

6.2. Fingerprints

The EU legal framework requires fingerprints as the secondary biometric to be introduced in e-passports. Its standard should be compliant with:

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004;
- ISO/IEC 19794-4:2005, Biometric Data Interchange Formats – Part 4: Finger Image Data;
- ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"; FBI: Wavelet Scalar Quantization (WSQ).

The primary fingerprints to be incorporated into the EU e-passports shall be plain impressions of the left and right index finger.

In the case of insufficient quality of the fingerprints and/or injuries of the index fingers, good quality, plain impressions of middle fingers, ring fingers or thumbs shall be recorded (the storage format CBEFF – Common Biometric Exchange Format Framework) will record the type of fingers used (left index, right middle, etc.) in order to ensure verification with the correct finger.

The fingerprints must be stored as images according to ISO/IEC 19794-4:2005, the quality of the fingerprint images shall be according to the ISO standard mentioned and ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information". According to the latter a compression of the images using the WSQ-algorithm must be used in order to decrease the file size.

The use of fingerprint images requires approximately 12–15 Kbyte per finger.

6.3. Chip

Storage medium (RF-Chip architecture) should have a standard compliance with:

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Document, Technical Report, Version 2.0, 05 May 2004;
- ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards;
- ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 April 2003.

According to the above-mentioned documents, both type A and type B RF-interfaces are considered to be ICAO Standard compliant.

ICAO compliant passports will be equipped with either A or B type RF interfaces, requiring border inspection systems to accommodate both standards for passports.

According to the ICAO Logical Data Structure [12], alphanumeric data of the MRZ of the document and digital document security data (PKI) must be stored on the chip together with the biometric identifiers.

On the EU level, the states are required to use appropriately sized RF chips to hold the personal data and biometric features according to the Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by the Member States.

The alphanumeric data, printed in the MRZ of the passport, according to ICAO Doc 9303, Part 1 Machine Readable Passports, Sixth Edition, 2006 (remained draft in the text of the Annex), have to correlate to the data digitally stored in the chip according to ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, of 18 May 2004. Chip Logical Data Structure should be developed according to the latter.

6.4. Data security and integrity issues

The integrity, the authenticity and confidentiality of the data, digitally stored in the passport's chip, have to be equally secured. This requires the following mandatory/optional international standards on:

- Passive Authentication – required for all data (ICAO mandatory security feature);
- Active Authentication – optional;
- Chip Authentication – additional protection on the EU level required for all data at the time when fingerprint data are introduced or at the latest 36 months after the adoption of the technical specifications. Such a protection must not be enforced by the chip, but EU-Inspection systems must use this mechanism, if supported by the chip;
- Basic Access Control – required for all data;
- Terminal Authentication – additional protection required for fingerprint data.

For more information on this subject, the following documents should be consulted:

- ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004;
- ISO/IEC 7816-4:2005, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange;
- Advanced Security Mechanisms for Machine Readable Travel Documents, Version 1.0, 2005.

6.5. Requirements of the European Union for Public Key Infrastructure for Passports and Inspection Systems

In order to ensure integrity and authenticity of the digital data stored on the chip, a PKI is introduced:

Each EU Member State must set up only a single Country Signing CA acting as the national trust point for all receiving states and at least one Document Signer issuing passports. Details on this PKI infrastructure (including signature algorithms, key lengths, and validity periods) can be found in ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004.

To prevent unauthorized inspection systems to access fingerprint data, another PKI is introduced:

Each EU Member State must set up only a single Country Verifying CA acting as the national trust point for the passports issued by this Member State and at least one Document Verifier managing a group of authorized inspection systems. Details on this PKI infrastructure can be found in Advanced Security Mechanisms for Machine Readable Travel Documents, Version 1.0, 2005.

Conclusions

In the area of use of the biometrics the significant progress was reached during the last 5 years and it is widening in the daily life. The electronic passports with the biometrics are already in use in about 90 percent of ICAO Member States.

Although this article touched mainly the current technical solutions for the use of biometrics in passports; it shall not be forgotten, that in order to effectively implement these solutions and benefit from the results of such a use any state must comply with such criteria as:

- to have high level of personal data protection ensured,
- to have a modern civil register system,
- to have a proper equipment in place in order to capture, process and store the biometrics of the persons for the purpose of the issuance of passports,
- to have complex system to be used for the identification of the persons already having e-passports with biometrics (e.g. at the border crossing points),
- to ensure the complex approach to all the above mentioned components in order to treat them as one sophisticated public data management system.

Finally it is also very likely that based on the current experiences of the ICAO Member States, and, in particular those, which are also EU Member States, the new technical solutions will be elaborated by the international organizations in the long-term perspective.

References

1. *Council Regulation (EC) No 2252/2004* of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.
2. *Decision of the European Commission C(2006)2909* establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States.
3. *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 2252/2004* on standards for security features and biometrics in passports and travel documents issued by Member States (COM(2007) 619 final).
4. *Council Regulation 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation 2252/2004* on standards for security features and biometrics in passports and travel documents issued by Member States.

5. *Doc. 9303* of the International Civil Aviation Organization.
6. *Welcome to ICAO/MRTD* – http://mrtd.icao.int/content/view/33/202/, checked on 10.07.2009.
7. *ICAO MRTD Report* 2, No 1, 2007.
8. *ICAO MRTD Report* 4, No 1, 2009.
9. *According to ICAO standards*. Face biometric data interchange image recorded in Datagroup 2 of the LDS shall be derived from the passport photo used to create the displayed portrait printed on the data page of the Machine Readable Passport; and shall be encoded either according to full frontal image or token image formats set out in the latest version of ISO 19794-5.
10. *ICAO NTWG*, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004.
11. *ICAO NTWG*, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004.
12. *ICAO NTWG*, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004.

Received on the 21st of August, 2009