



1710/05/EN-rev  
WP 112  
04/09/12

**Opinion 3/2005**  
**on Implementing the 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**  
*(Official Journal L 385 , 29/12/2004 p. 1 - 6)*

**Adopted on 30 September 2005**

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

Website: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/index\\_en.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm)

Table of contents

Opinion on implementing the 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 (*Official Journal L 385 , 29/12/2004 P.1 - 6*) ..... 3

1. Introduction ..... 3
  - 1.1. General issue ..... 3
  - 1.2. History and background of Council Regulation (EC) No 2252/2004 ..... 4
  - 1.3. Previous Opinion of the Working Party ..... 5
  - 1.4. Resolution of the International Conference of Data Protection and Privacy Commissioners ..... 6
2. Implementation of biometric features in passports, other travel documents and ID-cards 7
  - 2.1. General considerations ..... 7
  - 2.2. Ethic risks of the use of biometric features in passports, other travel documents and ID-cards ..... 7
  - 2.3. Legislative aspects of the implementation of biometrics ..... 8
    - a) Reservations about a centralized European or national database on biometrics ..... 8
    - b) Access to biometrics for competent authorities only ..... 9
  - 2.4. Technical aspects ..... 9
    - a) Implementation of a digitalized facial image ..... 10
    - b) Implementation of additional biometric features particularly with regard to fingerprints ..... 11
3. Conclusions ..... 11

**Opinion 3/2005**  
**on implementing the 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**  
*(Official Journal L 385 , 29/12/2004 P.1 - 6)*

**THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH  
REGARD TO THE PROCESSING OF PERSONAL DATA**

**set up under Directive 95/46/EC of the European Parliament and of the Council of  
24 October 1995<sup>1</sup>,**

Having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,  
Having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

**HAS ADOPTED THE FOLLOWING OPINION:**

***1. Introduction***

**1.1. General issue**

In its “**Working document on biometrics**”<sup>2</sup> the Working Party stressed that “the rapid progress of biometric technologies and their expanded application in recent years necessitates careful scrutiny from a data protection perspective. A wide and uncontrolled utilisation of biometrics raises concerns with regard to the protection of fundamental rights and freedoms of individuals. This kind of data is of a special nature, as it relates to the behavioural and physiological characteristics of an individual and may allow his or her unique identification.”

Since these fundamental comments on biometrics the legislative developments have proceeded rapidly. The European Council of Thessaloniki, on 19 and 20 June 2003, confirmed that a coherent approach is needed in the European Union on biometric identifiers or biometric data for documents for third country nationals, European Union citizens’ passports and information systems (VIS and SIS II). In autumn 2003 the European Commission submitted a draft Council Regulation amending Regulations 1683/95 and 1030/2002 laying down a uniform format for visas and for residence permits for third country nationals respectively.

---

<sup>1</sup> Official Journal no. L 281 of 23/11/1995, p. 31, available at:  
[http://europa.eu.int/comm/justice\\_home/fsj/privacy/law/index\\_en.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm).

<sup>2</sup> MARKT/10595/03/EN – WP 80, adopted 1 August 2003.

## **1.2. History and background of Council Regulation (EC) No 2252/2004**

On 18 February 2004 the European Commission submitted a draft Regulation on standards for security features and biometrics in EU citizens' passports<sup>3</sup>. The aim of the proposal was to render passports more secure by means of a legally binding instrument on standards for harmonised security features and at the same time to establish a reliable link between the genuine holder and the document by introducing biometric identifiers. In addition, this would allow EU Member States to meet the requirements of the US Visa waiver programme in conformity with international standards. In this draft the European Commission proposed that passports and other travel documents should include a storage medium with a facial image in a mandatory manner. The Member States were allowed to implement fingerprints into the passports by national law. Furthermore the European Commission proposed that the biometric identifier shall be stored on a storage medium with sufficient capacity. It could be a contactless chip but it may also be another storage medium with the capacity required, details to be determined by the technical experts in the responsible committee. The draft Regulation also offers the possibility to store fingerprints in a national database with a view to a future European Register of issued documents.

In summer 2004 the proposal had been discussed in the Visa Working Party. On 6 October 2004 the SCIFA (Strategic Committee on Immigration, Frontiers and Asylum) finally discussed the proposal and submitted it to the European Parliament. The final proposal thus envisaged the digital facial image as the first biometric feature in a mandatory manner and fingerprints as a second biometric feature in a facultative way.

As a result a of the JHA (Justice and Home Affairs) Council on 25-26 October 2004 the text of the proposal was changed to envisage both biometric features in a mandatory way<sup>4</sup>.

The European Parliament's non-binding legislative resolution on the Commission proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports from 2 December 2004<sup>5</sup> was adopted by 471 votes in favour to 118 against and 6 abstentions. The Parliament is supporting the introduction of passports containing a facial image on the ground that this biometric element will make it more difficult to falsify passports. The biometric data, it is reasoning, will ensure that a person presenting a passport is in fact the person to whom the passport was originally issued. Pleading that the implementation of biometric elements must not infringe upon privacy and data protection rights, it rejected the mandatory inclusion of fingerprints and the creation of a central database of EU passports and travel documents. The legislative resolution of 2 December 2004 declares that the biometric features in passports shall only be used for verifying the authenticity of the document and the identity of the passport holder and that they shall be stored on "a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored". The resolution also states that only the authorities of the Member States who are competent for reading, storing, modifying and erasing the biometric data may have access to it. Furthermore, the

---

<sup>3</sup> Document COM(2004)116-final, noted in Official Journal no. C 98 of 23 April 2004, p. 39.

<sup>4</sup> Council Document 15139/2004.

<sup>5</sup> European Parliament legislative resolution on the proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), <http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN&LEVEL=2&NAV=X>.

Parliament introduces an amendment to the draft Regulation text specifically stipulating that “no central database of European Union passports and travel documents containing all EU passport holders' biometric and other data shall be set up”. According to the report of the Committee on Civil Liberties, Justice and Home Affairs of 25 October 2004, “the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets.”

The Council adopted Regulation (EC) No 2252/2004 on standards for security features and biometrics in travel documents issued by Member States on 13 December 2004 on the basis of the draft of the JHA Council of 25-26 October 2004<sup>6</sup>. The Council Regulation envisages the digital facial image as a first biometric feature in a mandatory manner and fingerprints as a second biometric feature also in a mandatory way. The Council did not take account of the suggestions and requests of change laid down by the Parliament. According to its Article 6 the Regulation entered into force on 18 January 2005. In that same Article 6 the Regulation rules that Member States shall apply the Regulation:

“(a) as regards the facial image: at the latest 18 months

(b) as regards fingerprints: at the latest 36 months,

following the adoption of the measures referred to in Article 2.”

On 28 February 2005 the European Commission passed the “Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States”<sup>7</sup> which refer to Article 2 of the Council Regulation (EC) No 2252/2004.

### **1.3. Previous Opinion of the Working Party**

The Chairman of the Article 29 Working Party on 18 August 2004 addressed a letter to the President of the European Parliament, the President of the LIBE Committee, the Secretary General of the Council of the European Union, the President of the European Commission, the Director General of DG Enterprise and the Director General of DG Justice and Home Affairs. He pointed to the following concrete proposals.<sup>8</sup>

“1. The Working Party strictly opposes the storage of all EU passport holders' biometric and other data in a centralised data base of European passports and travel documents.

2. The purpose of introducing biometric features in passports and travel documents as defined by the Regulation has to be explicit, appropriate, proportionate and clear.

---

<sup>6</sup> Official Journal no. L 385 p. 1-6, published 29 December 2004.

<sup>7</sup> C(2005) 409 final, (not yet published in the Official Journal).

<sup>8</sup> Letter of the Chairman of the Art. 29 Working Party to the President of the European Parliament, the President of the LIBE Committee, the Secretary General of the Council of the European Union, the President of the European Commission, the Director General of DG Enterprise and the Director General of DG Justice and Home Affairs, dated the 18 August 2004 (not published).

3. The Member States should guarantee in a technically sound way that the passports include a storage medium with sufficient capacity and the capability to guarantee the integrity, the authenticity and the confidentiality of the data.
4. The Regulation should define who may have access to the storage medium and for which purposes (reading, storing, modifying or erasing data).
5. The Member States shall set up a register of competent authorities.”

The Chairman pointed out that the security features on passports and travel documents have to be valid and guaranteed for the whole period of validity of the document. The issuing entities are responsible for the security standards and the necessary infrastructure. Citizens can not be blamed for any lapses in this field occurring in the process of editing and issuing the document or during its period of validity.

Finally he drew the attention to the Opinion on biometrics (WP 80) which was adopted by the Working Party on 1 August 2003<sup>9</sup> and to the Opinion on biometric features in visas and residence permits (WP 96) adopted on 11 August 2004<sup>10</sup>.

In a further letter of 30 November 2004 addressed to the President of the LIBE Committee and to the President of the Council of the European Union the Chairman of the Article 29 Working Party argued against a second mandatory biometric feature. The Chairman stressed that the introduction of an additional biometric feature makes it all the more necessary to create a secure and waterproof system making sure that the fundamental right of privacy is not endangered.

In this regard consideration must also be taken of the recent Opinion of the Art. 29 Working Party(WP110) of 23 June 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final).<sup>11</sup> This Opinion reminds the position of the Art. 29 WP on biometrics and requests for the setting up of appropriate safeguards for the processing of biometric data in the VIS.

#### **1.4. Resolution of the International Conference of Data Protection and Privacy Commissioners**

On 16 September 2005 the 27th International Conference of Data Protection and Privacy Commissioners in Montreux adopted the **Resolution on the use of biometrics in passports, identity cards and travel documents**.<sup>12</sup> In this Resolution the International Conference is pointing out that the widespread use of biometrics will have a far-reaching impact on the global society and therefore should be subject to an open worldwide debate. The International Conference is calling for

1. effective safeguards to be implemented at an early stage to limit the risks inherent to the nature of biometrics,

---

<sup>9</sup> MARKT/10595/03/EN – WP 80, adopted 1 August 2003.

<sup>10</sup> MARKT/11224/04/EN – WP 96, adopted 11 August 2004.

<sup>11</sup> MARKT/1022/05/EN.

<sup>12</sup> <http://www.privacyconference2005.org> (not yet published).

2. the strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations and for contractual purposes on the basis of consent,
3. the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder when presenting the document.

## ***2. Implementation of biometric features in passports, other travel documents and ID-cards***

Article 1 par. 2 of Regulation (EC) No 2252/2004 provides a digitalized facial image and fingerprints as biometric features in the EU citizens' passports in a mandatory manner. Pursuant to its Article 6 and according to the European Commission Decision C (2005) 409 of 28 February 2005 the Member States will have to implement the digitalized facial image into the passports of their citizens by 28 August 2006 and the fingerprints by 28 February 2008. The first Member States will have to start to issue so called ePassports with a digitalized facial image stored in a RFID-chip in autumn 2005. In Member States issuing ID-cards there are ideas to implement biometric features into them.

### **2.1. General considerations**

The introduction of biometric features into passports will have far reaching consequences for the holders of the passports. Hence it cannot be done without a proper assessment of the impacts on privacy. Up to now it was adequate to have a description of some biometric features in passports or other travel documents such as a photo, description of sex, height, or colour of the eyes. After implementation of Council Regulation (EC) 2252/2004 the European citizens will have to provide biometric data in a digital way. These data can be stored in databases and they can be made available to a lot of not predictable purposes.

### **2.2. Ethic risks of the use of biometric features in passports, other travel documents and ID-cards**

There are quite a lot of ethic risks as regards the implementation of biometric features in passports, other travel documents and ID-cards. Funded by the EC in the scope of the Sixth Framework Programme for Research and Technological Development (FP6) the BITE-Project (biometric identification technology ethics) started in October 2004<sup>13</sup>. The objectives of BITE are to prompt research and to launch public debate on bioethics of biometric technology. A public consultation will be launched in June 2006. Another project supported by the European Union under the FP6 is FIDIS<sup>14</sup> (Future of Identity in the Information Society), carried out by a consortium of European universities and companies as well as further public and private institutions. The aim of FIDIS is shaping the requirements for the future management of identity in the European Information Society and contributing to the technologies and infrastructures needed.<sup>15</sup>

---

<sup>13</sup> <http://www.biteproject.org/>

<sup>14</sup> <http://www.fidis.net>

<sup>15</sup> Two other projects, BIOSEC and BIOSECURE, funded by the FP6 as well explore also this issue to a certain extend. <http://www.biosec.org> and <http://www.biosecure.info>

According to a prospective study<sup>16</sup> commissioned by the LIBE committee of the European Parliament, fallback procedures should be available to constitute essential safeguards for the introduction of biometrics as they are neither accessible to all nor completely accurate. Such procedures should be implemented and used in order to respect the dignity of persons who could not follow successfully the enrolment process and to avoid transferring onto them the burden of the system imperfections.<sup>17</sup>

One of the aspects of the discussion is that governmental institutions and other public authorities will be able to collect and store a huge number of sensitive information about their citizens. In this context it should be particularly pointed out that collecting biometric features means collecting data of the *body* of a person.

Another aspect is that up to now biometric features, like fingerprints, have mostly be collected in criminal cases. The question is: Will the European citizens be prepared to give their fingerprints for other purposes ?

Other concerns are of a diverse nature: Persons to whom it might be more difficult to prove their identity, such as immigrants, may be unjustly targeted under such a system; disabled people who are unable to undergo biometrics tests may become stigmatized; and sensitive medical information may be obtainable. On a practical level, privacy laws are differing from country to country, which will have implications for the sharing of data and the interrelation of databases.

In the case of storing fingerprints attention will have to be paid in so far as various correlations between certain papillary patterns and corresponding diseases are discussed. As for instance certain papillary patterns are said to depend on the nutrition of the mother (and thus of the foetus) during the 3rd month of the pregnancy<sup>18</sup>. Leukaemia and breast cancer seem to be statistically correlated with certain papillary patterns. Any direct or precise correlations in these cases are not known, though. But there is an ongoing scientific discussion which cannot be disregard.

### **2.3. Legislative aspects of the implementation of biometrics**

#### **a) Reservations about a centralized European or national database on biometrics**

In the legislative decision on 2 December 2004 the European Parliament required the prohibition of a central database of European Union passports and travel documents containing the biometric and other data of all EU passport holders. The Working Party supports this demand and states that the objection against a European central database of European Union passports and travel documents are the same objections against national central databases of passports and travel documents as well as against central databases for ID-cards.

There is a risk that the setting up of a centralized database containing personal data and in particular biometric data of all (European) citizens could infringe against the basic principle

---

<sup>16</sup> Biometrics at the frontiers: assessing the impact on Society, February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, European Commission.

<sup>17</sup> Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, Council of Europe, 2005., page 11

<sup>18</sup> FIDIS, Study on PKI and biometrics, p. 68.



of proportionality. Any central database would increase the risks of misuse and misappropriation. It would also intensify the dangers of abuse and function creep. Finally, it would raise the possibilities of using biometric identifiers as 'access keys' to various databases, thereby interconnecting data sets.

#### **b) Access to biometrics for competent authorities only**

The biometric features in the passports, in any other travel documents or in ID-cards are of high sensitivity. Thus it has to be guaranteed that only competent authorities are able to have access to the data stored in the chip. Any unauthorised access will not be acceptable. For this purpose the Working Party supports the European Parliament's demands that each Member State shall maintain a register of the competent authorities and authorised bodies referred to in Article 3 of Regulation (EC) 2252/2004. The Member States shall communicate this register and, if necessary, regular updates thereof to the Commission, which shall maintain an up-to-date online register and which shall publish a compilation of the national registers every year.

In case of any rejection in border checks or other checks made by competent authorities, the respective persons must be informed of the reasons of the rejection, the means by which they can assert their own points of view and the competent authorities for appeal.

#### **2.4. Technical aspects**

The technical risks are of a diverse kind. The risks are concerning the implementation of a contactless chip (RFID-chip) as well as the implementation of biometric features contained in that chip.

In its legislative decision of 2 December 2004 the European Parliament required that the passport shall include a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored. The Working Party was in support of this demand<sup>19</sup>, but this was not taken into account by the Council. The RFID-chip according to ISO-standard 14443 which the Regulation of 13 December 2004 is envisaging creates a lot of risks for the right of privacy of the European citizens. The Commission decision of 28 February 2005<sup>20</sup> is not appropriate to safeguard the rights of the citizens, since the contact between the RFID-chip and the reader can be eavesdropped and the information can be skimmed.

The risks stemming from the implementation of RFID-chips in the passports, in other travel documents or in ID-cards as well as the risks arising from the implementation of biometric features in the chip need a security architecture which is aimed at providing an increased level of confidence for information to be exchanged. Fully aware of the inherent problems the Working Party thus sees a need for a global Public Key Infrastructure (PKI). Public key certificates contain information about the holder. Each digital certificate can be traced uniquely to the person to whom it has been issued. Digital certificates are as unique as are social security numbers, credit card numbers or health registration numbers. But digital certificates can be misused to deny a certificate holder access to services. In addition to that,

---

<sup>19</sup> Letter of the Chairman of the Art. 29 Working Party to the President of the European Parliament, the President of the LIBE Committee, the Secretary General of the Council of the European Union, the President of the European Commission, the Director General of DG Enterprise and the Director General of DG Justice and Home Affairs, dated the 18 August 2004 (not published).

<sup>20</sup> C(2005) 409 final.

transaction generated data conducted with target certificates can be filtered out by surveillance tools, and delivered electronically to third parties or to the police or other authorities.

For these risks it is mandatory to create a Protection Profile (PP) according to the Common Criteria for Information Technology Security Evaluation (Common Criteria – CC) vers. 2.1 (ISO-standard 15408). They provide a generally accepted solution for IT-security problems. Protection Profile describes an IT-security concept which has to be complete, consistent and coherent. The Protection Profile should be submitted by the Committee set up by Article 5 of Regulation (EC) No 2252/2004. In accordance with the requests submitted by the European Parliament as regards changes in its legislative resolution of 2 December 2004 the Working Party suggests that the Committee should be assisted by experts appointed by the Working Party.

#### **a) Implementation of a digitalized facial image**

According to the European Commission's Decision of 28 February 2005 Member States are committed to implement a digitalized facial image into the passports of their citizens by 28 August 2006. Pursuant to Article 1 and to Nr. 5.2 of the Appendix of the Decision to Member States have to secure the access to the data in the chip by a security feature called Basic Access Control (BAC). BAC is a recommendation of the International Civil Aviation Organisation (ICAO), but it is not mandatory<sup>21</sup>. The goal of the BAC mechanism is to prevent skimming as well as eavesdropping. It shall guarantee that access to the data and to the biometric data in particular is possible only when before reading the data from the chip a 'Document Basic Access Key' had been build from the machine readable zone (MRZ) of the passport by an optical contact between passport and reader. The 'Document Basic Access Key' is calculated from the number of the passport, the date of birth and the date of expiry. After building the 'Document Basic Access Key' the reader is in the position to read the data which are stored in the RFID-chip. For security purposes the transmission of the data takes place in an encrypted manner. This implies a certified security-chip with an encrypted co-processor.<sup>22</sup>

BAC does not represent an adequate security feature, though. It bases on the Machine Readable Zone (MRZ) of the passport. But the data in the MRZ are not handled in a strictly confidential manner. For example, if a European citizen wants to get a ticket for an outstanding event such as "2006 FIFA World Cup Germany" or "UEFA Euro 2008" in Austria and in Switzerland the citizen has to reveal name, date of birth, number of the passport or of the ID-card as well as the day of issue of the document into an internet form. These proceedings for getting a ticket have been already carried out for the "UEFA Euro 2004" in Portugal. They will be implemented furthermore at the occasion of some other events like concerts or other big sport events like the Olympic Games or athletics world championships. As in some Member States private companies are copying passports or ID-cards to secure outstanding debits, the constituent parts of the 'Document Basic Access Key' are not secret and it is to be feared that the algorithm of the BAC will be once available on the internet.

---

<sup>21</sup> ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, published 1 October 2004, page 16.

<sup>22</sup> For the purpose of safe transmission the so called Essen Group has developed a special software called Golden Reader Tool. The Essen Group is consisting of public authorities, IT-security companies and companies which produce travel documents from Germany, the Netherlands and the United Kingdom.

## **b) Implementation of additional biometric features particularly with regard to fingerprints**

The circumstances under which fingerprints are collected will have to guarantee perfect reliability. Whereas ICAO is regarding a digitalized facial image as not sensitive - because there is still a photo of the holder in the passport - it is recognizing that the implementation of fingerprints and other additional biometric features in the passport is of a highly sensitive nature. Hence ICAO is recommending a special security mechanism called Extended Access Control<sup>23</sup>. The Extended Access Control mechanism is working similar to the BAC mechanism as described above. However, for Extended Access Control a 'Document Extended Access Key' set is used instead of the 'Document Basic Access Keys'. Defining the (chip-individual) 'Document Extended Access Key' set is up to the implementing State. The 'Document Extended Access Key' set may consist of either symmetric keys, e.g. derived from the MRZ and a "National Master key", or an asymmetric key pair with a corresponding card certificate. But a lot of details of these security mechanisms are still unclear.

Extended Access Control is representing a progress as regards security measures, but this security mechanism is only optional as is the BAC<sup>24</sup>. Add to this it is a moot point whether Extended Access Control will be implemented by Non-Member States. The European Commission and the Member States should guarantee that passports of European citizens including data of fingerprints could not be read by readers that could not support Extended Access Control.

### **3. Conclusions**

The implementation of biometric features in passports, other travel documents and ID-cards raises a lot of ethic, legal and technical questions. Thus the Working Party is pointing to the following aspects:

1. Before implementing biometric features in passports, other travel documents or ID-cards there must be an exhaustive discussion in society. For this purpose it is necessary to await the outcomes of the BITE-project.
2. In order to limit the risks inherent to the nature of biometrics effective safeguards have to be implemented at an early stage. For this purpose the Committee set up by Article 5 of Regulation (EC) 2252/2004, which is to be assisted by experts appointed by the Article 29 Working Party, will have to present a Protection Profile.
3. The strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations on the one hand and those for contractual purposes on the basis of consent on the other hand must be guaranteed.
4. The use of biometrics in passports and identity cards has to be technically restricted for verification purposes comparing the data in the document with the data provided by the holder when presenting the document.

---

<sup>23</sup> ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, published 1 October 2004, page 17.

<sup>24</sup> ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, published 1 October 2004, page 17, 21 and 22.

5. The European Commission and the Member States should guarantee that passports of European citizens including data of fingerprints could not be read by readers that could not support Extended Access Control.

6. It should be guaranteed that only competent authorities are able to have access to the data stored in the chip. Member States shall set up a register of competent authorities.

Done at Brussels, on 30 September 2005

For the Working Party  
The Chairman  
Peter Schar