

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 18.2.2004
COM(2004) 116 final

2004/0039 (CNS)

C5-0101-04

Proposal for a

COUNCIL REGULATION

on standards for security features and biometrics in EU citizens' passports

(presented by the Commission)

EXPLANATORY MEMORANDUM

1. INTRODUCTION

At present, the commonly called "European Passport" is established on the basis of Resolutions on the introduction of a passport of uniform pattern[1]. This was adopted by the Representatives of the Governments of the Member States meeting within the Council considering that the creation of a uniform passport model "is likely to facilitate the free movement of nationals of Member States" and that they were "anxious to promote any measures which might strengthen the feeling among nationals of the Member State that they belong to the same Community"[2]. A Resolution on minimum security standards for the passport was adopted in October 2000.

Following the tragic events of 11 September 2001, there was a call for immediate reaction in enhancing security features in documents. Subsequently, the Commission presented three proposals: one, amending Regulation 1683/95 laying down a uniform format for visas introducing a photograph produced in accordance with high security procedures[3], a second introducing a uniform format for forms for affixing the visa issued by Member States to persons holding travel documents which are not recognised by the Member State drawing up the form[4], and thirdly on a uniform format for residence permits for third country nationals[5] in order to render the joint action legally binding, at the same time introducing the photograph of the holder into the sticker version of the permit. These proposals for Regulations were adopted in February and June 2002.

Already at the time of adoption of the above mentioned proposals, Member States saw a need to further enhance the security of travel documents by adding biometric elements. In a statement on the occasion of the informal ministers meeting in Santiago de Compostella on 14/15 February 2002, the Commission presented its willingness to act with a proposal if Member States would like it to do so, making clear that such a proposal would only concentrate on harmonising the security features in the passport and would not alter the layout in any way.

At the informal JHA Minister's meeting in Veria on 28/29 March 2003, Member States called again for a Commission proposal to integrate biometric identifiers into the uniform format for visas and residence permits for third country nationals. The Commission undertook to present a proposal, at the same time emphasising that a coherent approach should be taken in respect of all travel documents, including the passport of EU citizens.

The European Council of Thessaloniki confirmed that "a coherent approach is needed in the EU on biometric identifiers or biometric data for documents for third country nationals, EU citizen's passports and information systems (VIS and SIS II)", and invited the Commission "to prepare the appropriate proposals, starting with the visa".

---

1 OJ C 241, 19.9.1981, p.1
OJ C 179, 16.7.1982, p.1
OJ C 185, 24.7.1986, p.1
OJ C 200, 04.8.1995, p.1

2 OJ C 241, 19.09.1981, p. 1-7

3 Regulation 334/02: OJ L 53 of 23.02.2002 p.7

4 Regulation 333/02: OJ L 53 of 23.02.2002 p.4

5 Regulation 1030/02: OJ L 153 of 15.06.2002, p. 1

The first step has already been realised by the Commission by two proposals which were presented in September 2003 on the integration of biometric identifiers into the visa and the residence permit for third country nationals. As requested by the European Council of Brussels, a common approach on the latter proposals was reached in the Council on 27 November and at the same time, the mandate was given to the technical committee created by Article 6 of Regulation 1683/95 on a uniform format for visas to start working on the development of ways and means to implement these measures.

The European Council of Brussels on 12 December 2003 invited "the Commission to submit in due time a proposal for the introduction of biometric identifiers in passports."

Therefore, the second step of the implementation of the Thessaloniki conclusions, the harmonisation of the security features of the European passport including the insertion of biometric identifiers, will now be presented in order to reach a harmonised approach thus avoiding solutions in each Member State with a lack of interoperability.

In this framework, it is worth to mention that the United States have set the 26 October 2004 as the final date for a visa waiver country "as a condition for designation or continuation of that designation that it has a programme to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric identifiers that comply with applicable biometric identifiers standards established by the International Civil Aviation Organization".

While all Member States are preparing for the new requirements of the US Visa Waiver Programme, it is necessary to take a common approach towards the new United States legislation requiring biometric elements in passports of citizens of countries granted a visa waiver as from 26 October 2004.

2. AIM OF THE PROPOSAL

The proposal should aim at rendering the passport more secure by a legally binding instrument on minimum 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.

However, it is not the objective of the proposal to harmonise the layout of the passport format, neither to identify whether the passport has been issued to the right person in the first instance as only Member States can verify the identity of an applicant at the time of issuing the passport.

In relation to the first point, the minimum standards set out by the Resolutions seem not to reach sufficient harmonisation as they are subject to different use and interpretation of the security features. Member States will not integrate all elements and in any case during the set five year implementation delay, industry will have produced new security features, which will render the Resolution of 28 October 2000 out of date. Especially in relation to the photograph it can be noted that still 6 Member States affix the latter on the personal data page which presents a high risk for falsification as it can easily be substituted.

Another important reason for the Commission to bring forward enhanced common security standards is that the currently widely used travel documents should not lag behind those already achieved by fixing the technical specifications for the uniform format for visas and for residence permits for third country nationals. The standard of both uniform formats are constantly under review in order to keep the high quality in line with new developments and discoveries in the area of making documents more secure. The biometric identifiers for these documents have already been decided. In order to ensure coherence and to avoid that malafide persons will now turn to the less secured passport and identity card of EU nationals, the latter documents should also be upgraded in relation to their security. In accordance with the conclusions of the European Council of Thessaloniki this should happen in a harmonised and legally binding way. The above mentioned Resolution does not permit the type of flexibility and capacity of adaptation as provided for by this proposal for a regulation. Moreover, as these documents are produced under national competence some countries may lag behind others.

As a perspective, the prevention of fraudulent acquisition of documents such as passports, which is currently the responsibility of each issuing authority, would be enhanced. At EU level, a centralized, biometrics-based "EU passport register", which would contain the fingerprint(s) of passport applicants together with the relevant passport number and most probably some other, but limited, relevant data needed for a proper management of the system (see below point 8.), could be created.

In addition, this initiative will also be a significant measure in view of enlargement. The acceding states are currently changing their passport formats in order to make them more secure. They wish to bring them in line with the passports used within the European Union. A legally binding Regulation will give them the possibility to introduce the same security standards as the other Member States after accession. Finally, common security features will ease the control of the border police as at first sight, they can check some visible security features, present on all passports and only in doubtful cases they are bound to pursue a more in depth scrutiny. In case of a variety of security features, border police has to check each passport against 25 national passports containing different features and of different quality.

In relation to the second point, a proposal on the harmonisation of the security features including biometrics for the European passport would also have a big impact on our relations with third countries, for example the US. The biometrics integrated in the passport will correspond to ICAO (International Civil Aviation Organisation) recommendations and thus fulfil the requirements set out by the US for participation in its Visa Waiver programme. It would furthermore create a harmonised level of security in relation to European passports and thus not discard some EU citizens from benefits just because of their less secured national passports. A common effort could strengthen the European position towards the US.

3. LEGAL BASIS

It is necessary, as for the visa and the residence permit for third country nationals an enhanced level of document security has already been agreed, now to also render the passport more secure in order to prevent abuse of this -still less secured- document by malafide persons.

Indeed, its objective is to fight against the use of false documents. As passports are primarily controlled when crossing the external borders, the harmonisation of the security features of the European passport falls within the category of "standards and procedures" of border controls at the external borders. The harmonisation of the security features included in the

passports will obviously ease border controls as the border guards will immediately focus on the common standard features and not on individually used elements, differing from one Member State to the other. Furthermore the introduction of a biometric identifier, the facial image, will enable a thorough comparison of the person and the digital photograph at the border, which will in addition make border controls more efficient. Such a measure can be based on Article 62 (2) a) TEC.

In this respect, the legislative proposal should not go beyond the scope of this legal basis. The security of passports is important for reasons relating to external border controls: on the one hand, bona fide citizens will pass more smoothly through border controls; on the other hand, those who use forged or fraudulent passports will have less chance to enter the territory of Member States. This is based on two basic elements of our area of freedom and security. For these reasons this proposal is based on Article 62 (2) a).

In this context it should be noted that the acceding countries have requested to adapt the existing Resolutions on the passport (adopted by the Representatives of Member States meeting within the Council) in order to take on board the new languages which are currently not part of the Community languages and which are used for certain information in the passport. For reasons which lay in the scope of the offered legal basis, this appears not possible as the proposal is only about rendering the passport more secure by harmonising the security features and integrating one or more biometric identifiers. The same reasoning applies to a possible proposal for rendering the identity cards more secure. As stated above, the security of passports is important for reasons relating to external border controls.

4. CONSEQUENCES IN RELATION TO THE VARIOUS PROTOCOLS ANNEXED TO THE TREATY

Article 62 (2) a) TEC is used as a legal basis for the proposal and thus gives rise to the variable situation laid down by the protocols on the position of UK, IRL and DK. As an element of external border control and also being linked to visa policy this proposal should be considered as a development of the Schengen acquis with all the consequences resulting from this as regards the position of DK, ICL, NOR, UK and IRL.

As regards the Republic of Iceland and the Kingdom of Norway, the procedures laid down in the Association Agreement[6] concluded by the Council and concerning the latter's association with the implementation, application and development of the Schengen acquis are therefore applicable.

As an element of external border control and also being linked to visa policy this proposal should be considered as a development of the Schengen acquis. According to the special position of UK and Ireland as regards measures based on Title IV of the Treaty and Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland[7], and Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis[8] by which the present measure is not covered, the United Kingdom and Ireland do not take part in the adoption of the draft Regulation based on Article 62 (2) a) and are not bound by it or subject to its application.

---

6 OJ L 176, 10.7.1999, p. 36.
7 OJ L 131, 1.6.2000, p. 43.
8 OJL 64, 7.3.2002, p. 20.

Pursuant to the Protocol on the position of Denmark annexed to the TEU and the TEC, Denmark will not participate in the adoption of the Regulation and is therefore not bound by it or subject to its application. Given the fact that the draft Regulation is an act which aims to build upon the Schengen acquis in accordance with the provisions of Title IV of the TEC, Article 5 of the above-mentioned Protocol applies.

5. SUBSIDIARITY AND PROPORTIONALITY

Article 5 of the EC Treaty provides that "action by the Community shall not go beyond what is necessary to achieve the objectives of this Treaty". The form taken by Community action must be the simplest form allowing the proposal to attain its objective and to be implemented as efficiently as possible.

As an element of external border control and also being linked to visa policy this proposal should be considered as a development of the Schengen acquis, which should assure a harmonised application in all Member States applying the Schengen acquis. Therefore the form of a regulation has been chosen.

The harmonisation of document formats and of their security features will provide a guarantee against counterfeiting. By preventing forgery and counterfeiting of travel documents the Commission intends to enhance the high level of security, a target set out both by the Treaty and the European Council of Thessaloniki. This level of harmonisation can only be reached by Community action as already demonstrated by the adoption of several other instruments aiming at making documents more secure.

The proposal related to the integration of biometrics into the European passport intends to render it more secure, legally binding and easy adaptable to new circumstances given the risk of counterfeiting and forgery of this document, which should meet special situations for crossing of the external borders of the European Union and should therefore be the same throughout the EU. In addition it will provide for a reliable link between the document and its holder. The main reason for preferring a regulation to a directive is that the proposal provides for a total harmonisation of a minimum standard for the security elements of such documents, and their biometric identifiers, thus leaving no room for discretion to the Member States.

6. STRUCTURE OF THE PROPOSAL

The present Regulation is a first step and sets out the legal framework for a harmonisation of the security features and the introduction of biometric identifiers into the passport. A second step on the creation of a European Register for issued passports will follow in a longer term perspective.

The proposal provides for the minimum standard of security features to be introduced into the passport. Furthermore, it determines the biometrics to be used. Technical details have not been elaborated.

Implementation powers at the technical level in relation to the proposal should be delegated to the Commission with the assistance of the Committee created by Article 6 of Regulation 1683/95 laying down the uniform format for visas, in line with the procedure set out in Article

5 of Decision 1999/468/EC[9] in compliance with Article 7 thereof. This Committee will consequently be responsible for the security of all documents at EU level such as the uniform format for visa, residence permits for third country nationals and passports. Under this procedure possible technical specifications to implement the passport in accordance with the required security standards will be established. In relation to the biometric elements, it should decide for example on the development of a standard as regards the choice of the storage medium, its capacity and how to secure the stored information by using for example an appropriate PKI (**P**ublic **K**ey **I**nfrastructure) and digital signature. This will have the advantage that the needs can be identified by the technical experts and be adopted in a less time-consuming manner. The Committee can also take account more quickly of new technical developments.

7. MINIMUM SECURITY STANDARDS AND CHOICE OF THE BIOMETRICS

The Commission proposal is based on the security features which have been adopted by the Representatives of Member States meeting within the Council in its Resolution on minimum security standards for passports and other travel documents in October 2000. They are slightly "upgraded" in view of the technical developments in relation to visa and residence permits. It will render those features legally binding. The proposal will therefore set a harmonised high security standard for passports within the European Union including 25 Member States from 1 May 2004. Like in the Resolution, the Commission sets out the minimum standards and will not hinder Member States to go further if they wish to do so.

In accordance with the European Council conclusions of Thessaloniki, a coherent approach has to be taken as regards the introduction of biometric identifiers into the visa, the residence permit and the passport. The proposals in relation to visa and residence permits provide for two mandatory biometric identifiers: the facial image and fingerprints. Therefore the proposal for European passports could include the same mandatory biometric identifiers in order to ensure the coherence requested. However, coherence with the proposals on visa and residence permits of course does not necessarily mean that for each area, an identical solution should be adopted. The facial image is interoperable and can be used in our relations with third countries such as the US. However, the fingerprints could be added as an option for Member States who wish to do so, if they want to search in their national databases, which would be currently the only possibility for identification. This will change with the second step, the creation of the European Register for issued passports. In this case, the fingerprint has to be taken and registered in order to enable background searches (one-to-many).

When choosing the most appropriate biometric identifiers, the results of the work of the ICAO, which has taken the lead for the development of international standards in this respect and in the feasibility study on the visa information system (VIS), have been taken into account. It is also important not to lose sight of the need for a proper balance between the reinforcement of security and due regard for the individual rights of the persons concerned, notably the right to data protection and privacy, as guaranteed by Directive 95/46 EC and the national laws transposing it.

ICAO has also chosen the facial image as the primary interoperable biometric identifier and fingerprint and/or iris images as an optional biometric identifier for countries which require this for database searches.

---

9 OJ L 184, 17.7.1999, p. 23

The first biometric identifier, the high resolution electronic portrait, is already available in most passports. At borders, the electronic record could be used to display the image on the screen as well as the additional visual check, even if facial recognition technology is not applied. This would constitute a basic application of the digital photograph. A more advanced application would be the use of facial recognition systems with the digital photograph. This would require the availability of the necessary technology and equipment at the border crossing-point. The Commission leaves the choice to Member States whether they wish to display only the photo on the screen or run a facial recognition programme. The quality standards for the digital photograph set out by ICAO should be respected in order to ensure interoperability. The Commission leaves the choice of technology to Member States.

The storage of fingerprints either on the storage medium and/or in a national database is left at the discretion of Member States. However, if they register fingerprints it should be in interoperable formats as it would enable possible use via bilateral agreements between Member States. The access to such fingerprints could be administered by the introduction of Public/Private Key Infrastructure.

8. LONG TERM PERSPECTIVE: A EUROPEAN REGISTER FOR ISSUED PASSPORTS?

From a security point of view, in order to create the beginning of true "end-to-end" security, a centralised European register of issued passports (and possibly other documents used for travel purposes) could be created in a long term perspective. This register should then only include the fingerprint and the number of the travel document and no further personal data as its use should be limited to border controls in order to establish whether the travel document has been issued to the person present at the border in the first place.

It goes without saying that such a development needs to be further evaluated in order to assess the technical and legal impact and the cost-benefit ratio, especially in relation to the national issued passport registers which are currently developed in some Member States. Finally, it is of the utmost importance to examine the impact of the establishment of such a European Register on the fundamental rights of European citizens, and in particular their right to data protection.

9. SUPERVISORY AUTHORITIES ON DATA PROTECTION

The Regulation provides for the legal basis for Member States to store biometric data in the passport. The implementation of such action is left to the Member States in accordance with the technical specifications set out by the Committee created by Article 6 of Regulation (EC) 1683/95 on a uniform format for visas. Member States will carry out the processing of the biometric data.

Directive 95/46/EC on data protection[10] applies to the processing of personal data –including biometric data- by Member States' authorities within the scope of Community law.

In accordance with Article 28 of Directive 95/46/EC, Member States have established supervisory authorities that are responsible for the monitoring of the application within their territory of the provisions adopted by the Member States pursuant to Directive 95/46/EC.

[10] OJ L 281, 23.11.1995, p. 31

These authorities must act in complete independence when exercising the functions entrusted to them.

Those authorities are competent to hear claims on data protection lodged by any person or by an association representing that person.

They are endowed with

- Investigative powers, such as

– powers of access to data, forming the subject-matter of processing operations and

– powers to collect all the information necessary for the performance of their supervisory duties,

- Effective powers of intervention, such as,

– delivering opinions before processing operations are carried out, and

– ensuring appropriate publication of such opinions,

– ordering the blocking, erasure or destruction of data,

– imposing a temporary or definitive ban on processing, of warning or admonishing the controller,

– referring the matter to national parliaments or other political institutions,

- The power to engage in legal proceedings or to bring violations to the attention of the judicial authorities, where the national provisions adopted pursuant to Directive 95/46/EC have been violated.

Decisions by the supervisory authority, which give rise to complaints, may be appealed against through the courts.

Furthermore, those supervisory authorities have the obligation to draw up a regular report on their activities and may also be requested to exercise its powers by an authority of another Member State.

As already indicated in the explanatory memorandum of the recently presented Commission proposals on the introduction of biometric identifiers into the visa and residence permit for third country nationals, the supervisory authorities have a particular lack of resources.

Therefore it should again be underlined that when Member States implement the biometric identifiers in accordance with this Regulation, the above considerations must be taken into account. Measures aiming to reinforce public security must respect the fundamental rights and freedoms of the persons concerned. This implies in this context the increase of personnel in the national data protection supervisory authorities in order to ensure effective supervision and the choice of technologies, which comply with the provisions of Directive 95/46/EC. This is even more necessary when passports of their own nationals are concerned.

Consequently, the Commission also intends to submit this proposal to the Working Party set up by Article 29 of Directive 95/46/EC for consultation in accordance with Article 30 of the

said Directive as already done with the two proposals on the integration of biometrics into the visa and the residence permit.

However, when the European Register for issued passports is created the independent supervisory authority established by Regulation (EC) 45/2001 will have to take its responsibilities as regards the data protection issues.

10. FINANCIAL IMPACT

It is rather difficult to specify the exact financial impact of this legislative measure, as the exact requirements are not yet known and will be established by the Committee created by Article 6 of Regulation (EC) 1683/95 laying down a uniform format for visas.

In any event, it should be recalled that the photograph is already available in digital form for most of the passports as it is integrated in the personal data page; affixed photographs should no longer be used in new passports as it presents a security risk.

Furthermore, Member States are already actively working on improving the security level of their passports. They upgrade the security features and proceed with trials in biometrics in order to introduce biometrics into their passports with a view of complying with US Visa Waiver legislation.

For this reason, the present proposal will not add to the costs already foreseen by Member States for the improvement of their passport security.

In relation to the use of biometrics, the following technical requirements seem to be necessary:

– Storage medium

For the time being, the most appropriate storage medium is a contactless microchip. The microchip is necessary for the storage of the biometric information and the security code (PKI digital signature). ICAO recommends as a minimum standard a 32 K chip. However, as it may be necessary to store a facial image and fingerprint images, a 64 K chip would be more appropriate, especially if Member States wish to add some alphanumeric data.

The cost of such microchip is not yet known. The technology is developing rapidly and with the demand of chips needed for 25 Member States, prices should drop significantly. The Commission could also make a "grouped order" after a call for tender in order to obtain a better price.

– Enrolment equipment

Member States have to install enrolment equipment in the place where the data will be produced. Prices for enrolment equipment have dropped significantly over the past twelve months and are likely to drop further, which is why it is impossible to give a precise cost estimate for the mid-term future. Currently, appropriate European–made equipment for the enrolment of ten fingers (flat) costs roughly seven thousand euro.

– Verification systems

Verification systems have to be installed at border posts. Such equipments should be shared to achieve the verification of visas and acquired in the framework of the setting up of the VIS system provided that the implementation of biometrics is decided upon for the VIS. These devices can be used for all documents: visas, residence permits and passports.

11. COMMENTS ON THE ARTICLES

Article 1

Article 1 sets out the basic obligation of Member States to issue their passports following the minimum security standards referred to in the Annex to the Regulation.

The second sentence sets out the choice of the biometric identifier and allows the integration into the passport. It also specifies that the biometric identifier shall be stored on a storage medium with sufficient capacity. It could be a contactless chip but also another storage medium with the required capacity, to be determined by the technical experts in the responsible committee. It also gives the possibility to store the fingerprints in a national database in view of a future European Register of issued documents.

In case correction or deletions have to be made, for security reasons a new passport has to be issued.

The third sentence defines the scope of the documents to which the Regulation shall be applied.

Article 2

This Article confers the implementing powers as regards the Regulation to the Committee created by Article 6 of Regulation 1683/95 laying down a uniform format for visas.

The Committee establishes the possible necessary technical specifications linked to the security features of the passport, but also the additional technical specifications in relation to the integration of biometric identifiers.

This will ensure the necessary coherence and the possibility that the technical experts on this matter are able to co-ordinate the procedures and assume the responsibilities for all European Union documents in a satisfactory manner.

Article 3

Obviously some technical particulars should not be published under any circumstances in order to prevent such information being used for the purposes of counterfeiting or falsification. These technical particulars will therefore need to be laid down in a decision, since under Article 254 of the EC Treaty decisions do not need to be published. The Committee already equiped to deal with the uniform visa format will take decisions in this framework, since the same experts already have the relevant experience of very high technical standards, notably as regards safeguards against counterfeiting and falsification and secret documents.

For the same reasons, it is necessary to ensure that only persons so authorised by the Member States and Community bodies have access to this information. This also applies to the printing bodies, which are thus restricted in the first sentence of Article 3(2) to one per Member State.

Article 4

The Community is bound to respect fundamental rights such as protection of privacy, and data protection.

The wording of this article covers all applicable provisions on data protection: Directive 95/46/EC of the European Parliament and of the Council of 24.10.95 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[11]. It ensures that the person to whom the document has been issued is able to check the information introduced and that there is no other additional information provided.

The second sentence is necessary to allow the integration of biometric elements but limiting the personal data stored on the passport to those indicated either in the Regulation itself, its Annex or in the relevant passport of the person. It must be avoided that other information can be stored.

Article 5

This Article determines that the committee should carry out its tasks in compliance with the regulatory procedure set out in Article 5 of Decision 1999/468/EC in compliance with Article 7 thereof.

Article 6

This Article determines the implementation delay. It is set for one year after the adoption of the necessary technical specifications which will give Member States time to adapt their passports.

[11] OJ L 281, 23.11.1995, p. 31

2004/0039 (CNS)

Proposal for a

COUNCIL REGULATION

on standards for security features and biometrics in EU citizens' passports

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 62 (2) a) thereof,

Having regard to the proposal from the Commission[12],

Having regard to the opinion of the European Parliament[13],

Whereas:

(1) The European Council of Thessaloniki confirmed that a coherent approach is needed in the EU on biometric identifiers or biometric data for documents for third country nationals, EU citizen's passports and information systems (VIS and SIS II).

(2) Minimum security standards for passports were introduced by a Resolution of the Representatives of the Governments of the Member States meeting within the Council on 17 October 2000[14]. It is now appropriate to replace and upgrade this Resolution by a Community measure in order to achieve enhanced harmonised security standards for passports to protect against falsification. At the same time biometric elements should be integrated in the passport in order to establish a reliable link between the genuine holder and the document.

(3) The harmonisation of security features and the integration of biometric identifiers is an important step towards the use of new elements in the perspective of future developments at European level, which render the travel document more secure and establish a more reliable link between the holder and the passport as an important contribution to ensuring that it is protected against fraudulent use. The specifications set out in the document No 9303 on machine readable travel documents from the International Civil Aviation Organisation should be taken into account.

(4) This Regulation only should lay down such specifications that are not secret. These specifications need to be supplemented by specifications which are to remain secret in order to prevent the risk of counterfeiting and falsifications. Such additional technical specifications should be adopted in accordance with Council Decision 1999/468EC of

---

12 OJ C […], […], p. […].
13 OJ C […], […], p. […].
14 OJ C 310, 28.10.2000, p.1

28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission.

(5) The Commission should be assisted by the Committee established by Article 6 of Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas.

(6) In order to ensure that the information referred to is not made available to more persons than necessary, it is also essential that each Member State should designate not more than one body having responsibility for producing the passport, with Member States remaining free to change the body, if need be; for security reasons, each Member State must communicate the name of the competent body to the Commission and the other Member States.

(7) With regard to the personal data to be processed in the context of the passport, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[15] applies. It must be ensured that no further information shall be stored in the passport unless provided for in the regulation, its annex or unless it is mentioned in the relevant travel document.

(8) In accordance with the principle of proportionality, it is necessary and appropriate for the achievement of the basic objective of introducing common security standards and interoperable biometric identifiers to lay down rules for all Member States implementing the Schengen Convention. This Regulation does not go beyond what is necessary in order to achieve the objectives pursued in accordance with the third paragraph of Article 5 of the Treaty.

(9) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark does not take part in the adoption of this Regulation and is therefore not bound by it or subject to its application. However, given that this Regulation aims to build upon the Schengen acquis under the provisions of the third part of Title IV of the Treaty establishing the European Community, Denmark will, in accordance with Article 5 of the said Protocol, decide within a period of six months after the Council has adopted this Regulation whether it will transpose it into its national law

(10) This Regulation constitutes a development of provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis; the United Kingdom is therefore not taking part in its adoption and is not bound by it or subject to its application.

(11) This Regulation constitutes a development of provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of

---

15 OJ L 281, 23.11.1995, p. 31

the Schengen acquis*;* Ireland is therefore not taking part in its adoption and is not bound by it or subject to its application.

(12) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1, point B of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[16].

(13) This Regulation constitutes an act building on the Schengen *acquis* or otherwise related to it within the meaning of Article 3(1) of the Act of Accession.

HAS ADOPTED THIS REGULATION:

Article 1

1. Passports issued by Member States to their nationals shall comply with the minimum security standards set out in the Annex.

2. The passport shall include a storage medium with sufficient capacity, which shall be highly secured and shall contain a facial image. The Member States may also include fingerprints in interoperable formats.

3. This Regulation applies to ordinary passports, official passports (e.g. service passports and diplomatic passports), short term passports with a validity of more than six months, documents in lieu of passports issued as travel document in form of a passport booklet and travel documents issued by Member States to third country nationals or stateless persons.

Article 2

1. Additional technical specifications for the passport relating to the following shall be established in accordance with the procedure referred to in Article 5 (2):

(a) additional security features and requirements including enhanced anti-forgery, counterfeiting and falsification standards;

(b) technical specifications for the storage medium of the biometric information and its securisation;

(c) requirements for the quality and common standards for the facial image and the fingerprints.

[16] OJ L 176, 10.7.1999, p. 31

Article 3

1. The specifications referred to in Article 2 shall be secret and not be published. They shall be made available only to the bodies designated by the Member States as responsible for the printing and to persons duly authorised by a Member State or the Commission.

2. Each Member State shall designate one body having responsibility for producing the passport. It shall communicate the name of that body to the Commission and the other Member States. The same body may be designated by two or more Member States. Each Member State shall be entitled to change its designated body. It shall inform the Commission and the other Member States accordingly.

Article 4

1. Without prejudice to data protection rules, persons to whom the passport is issued shall have the right to verify the personal data contained in the passport and, where appropriate, to ask for any rectifications or erasure to be made.

2. No information in machine-readable form shall be included in the passport, unless provided for in this Regulation, or its Annex, or unless it is mentioned in the passport.

Article 5

1. The Commission shall be assisted by the Committee set up by Article 6(2) of Regulation (EC) No 1683/95.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply. The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at two months.

3. The Committee shall adopt its rules of procedure.

Article 6

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

The Member States shall apply this Regulation at the latest one year following the adoption of the measures referred to in Article 2. However, the validity of passports already issued shall not be affected.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

Done at Brussels, […]

For the Council
The President
[…]

ANNEX

Minimum security standards of the EU citizen's passport

1. Material

The paper used for those sections of the passport giving personal particulars or other data shall meet the following minimum requirements:

- no optical brighteners,

- duo-tone watermarks,

- security reagents to guard against attempts at tampering by chemical erasure.

- coloured fibres (partly visible, partly fluorescent under UV light)

- UV-fluorescent planchettes

- the use of security thread is recommended

If the personal data page is in sticker form, the watermark can be dispensed within the paper used for that page. The watermark can be dispensed within the paper used for the inside of the passport covers. Security reagents are required on the inside covers only if data are entered there.

If a card for inserting personal data in the passport is made entirely of plastic, it is not usually possible to incorporate the authentication marks used in passport paper. In the case of stickers and cards, the lack of marks in the materials shall be compensated for by measures in respect of security printing, use of OVDs (OVD = optically variable device), or an issuing technique over and above the following minimum standards.

2. Personal data page (second page of the passport)

The passport shall contain a machine readable personal data page, which shall comply with ICAO-Document 9303 on machine readable passports (Part 1) and the way it is issued, with the specifications for machine-readable passports set out therein.

The photograph of the holder shall also appear on this page and shall not be affixed but integrated into the material of the personal data page by the issuing techniques as referred to in No 5 of this annex.

3. Printing techniques

The following printing techniques shall be available:

- Background printing:

two-tone guilloches,

fluorescent rainbow colouring,

UV-fluorescent overprinting,

effective anti-counterfeiting and falsification motifs (especially on the biographical data page) with optional use of micro-printing,

reagent inks must be used on paper passport pages and stickers.

The lay-out of the biographical data pages shall be such that they are distinguishable from the other pages.

- *Form printing*:

with integrated micro printing (unless already included in background printing).

- *Numbering*:

On all pages inside the passport, printed (where possible with a special style of figures or typeface and in UV-fluorescent ink), perforated or in passport cards integrated using the same technique as for the biographical data. If a sticker is used for biographical data, printed numbering using fluorescent ink and a special style of figures is obligatory.

If stickers or non-laminated paper inside pages are used for biographical data, intaglio printing with latent image effect, micro text and optically variable ink shall also be employed. Additional optically variable security devices shall also be used on passport cards made entirely of plastic, at least through the use of optically variable ink or equivalent measures.

4. Protection against copying

An optically variable (OVD) or equivalent device, which provides for the same level of identification and security as currently used in the uniform format for visas shall be used on the personal data page and shall take the form of diffractive structures which vary when viewed from different angles (DOVID: Diffractive Optically Variable Image Device) incorporated into the hot-sealed laminate or as an OVD overlay, or, on stickers or a non-laminated paper inside page, as metallised or partially de-metallised OVD (with intaglio overprinting) or equivalent devices.

The OVD devices should be integrated into the document as an element of a layered structure effectively protecting against forgery and falsification: in documents made of paper, they should be integrated over the entire surface as an element of the hot-sealed laminate or security overlay, as described in Section 4; in documents made of plastic, they should be integrated in the card layer over as wide a surface as possible

If a plastic card is personalised by laser engraving and a changeable laser image (CLI) is incorporated therein, a diffractive OVD shall be applied, at least in form of a positioned metallised DOVID to achieve an enhanced protection against reproduction.

5. Issuing technique

To ensure that passport data are properly secured against attempts at counterfeiting and falsification, personal data including the photograph, the holder’s signature and main issue data shall in future be integrated into the basic material of the document. Conventional methods of attaching the photograph shall no longer be used.

The following issuing techniques may be used:

laser printing with document quality ink,

thermo-transfer,

ink-jet printing,

photographic,

laser engraving, that effectively penetrates into the card layers bearing the security characteristics.

To ensure that biographical issue data are adequately protected against attempts at tampering, hot-seal lamination with OVD security laminate is compulsory where laser printing, thermo-transfer or photographic techniques are used. In any event, an inside cover page should no longer be used for biographical data.

EU travel documents must be issued in machine-readable form. The layout of the biographical data page must follow the specifications given in ICAO Document 9303, Parts 1 and 3, and the issuing procedures must meet the specifications it sets for machine-readable documents. In passports, the inside cover page should not be used for biographical data.

Remark:

The most effective method of protecting against the illegal issue of stolen blank passports is to centralise the issuing procedure. Where passports continue to be issued on a regional or decentralised basis, appropriate security measures shall be taken in terms of logistics, administration and issuing techniques. This applies particularly to the storage of blank passports and of the material used for filling them in. With suitable programming, computerised issuing systems can also be used to authenticate passport issue (“electronic seal”).