STUDY FOR THE EXTENDED IMPACT ASSESSMENT OF THE VISA INFORMATION SYSTEM

FINAL REPORT

DECEMBER 2004

EPEC
Brussels Contact Address:
22-28 Avenue d'Auderghem
B-1040 Brussels
Belgium
Tel: +322 7402729
Fax: +322 7402720
www.epec.info

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The establishment of a visa information system (VIS) is one of the key initiatives in the European area of freedom, security and justice. Bearing in mind the important political, social and financial implications, it was decided that this initiative should undergo an extended impact assessment (EIA). This report presents the final results of the study conducted by European Policy Evaluation Consortium (EPEC, www.epec.info), on the basis of which the European Commission will draw up the EIA to accompany the legislative proposal for the VIS.

The study was based on desk research, consultations with Commission services, and a review of results of consultations with Member States and online public consultation. The main aims of the study were to:

- Elaborate current problems in relation to implementation of visa policy;
- Assess the fit between political objectives of VIS and current problems; and
- Assess the costs and benefits of policy options available to address the problems identified in the current situation.

Ultimately, the purpose of this exercise is to inform policy makers of the implications of choosing a particular course of action, and improve the transparency of policy-making. It is not, however, the task of the present study to make conclusions as to the choice of particular policy.

Schengen States[1] have developed a common visa policy, whereby they issue uniform short-stay visas to third country nationals which allow them to travel freely in the whole Schengen area. There are harmonised criteria and conditions for the issue of a Schengen visa, which is also in a uniform format.

Currently there are about 12 million Schengen visa applications (2001 data), of which 25% do not lead to visas being issued. It is projected that the numbers of visa applications will grow to 20 million visa applications in 2007. At the moment, citizens from 134 countries are required to apply for a visa before entering the territory of Schengen states.

One of the problems in the implementation of a common visa policy is that information from the visa application is routinely held only by the Member State which issued the visa. If a bona fide traveller applies for a Schengen visa again, but to the authorities of another Member State, the record of his past visa application is not readily available to the consular authorities of that Member State. There is some important exchange of visa data in the current situation, but it is partial, inefficient and time consuming.

[1] Belgium, Denmark, Germany, Greece, Spain, France, Italy, Luxembourg, Netherlands, Austria, Portugal, Finland and Sweden as well as Iceland and Norway. Ireland and the United Kingdom do not participate in the Schengen *acquis* concerning the lifting of internal border controls and the common visa policy and have thus not ended border controls with other EU Member States. In accordance with the Protocol on the position of Denmark, Denmark can choose within the EU framework whether or not to implement any new measure building on the Schengen *acquis* in its national law.

In addition, there are problems with the implementation of the Dublin II Regulation, which determines the Member State responsible for the examination of an asylum claim. One of the criteria for this decision is the provision that the Member State issuing the visa, is also responsible for the examination of asylum claim. At the moment Member States do not have an efficient means to check whether an asylum seeker was issued a visa by another Member State.

Thessaloniki European Council of 5 June 2003 called for a coherent approach in the EU on biometric identifiers or biometric data, which would result in harmonised solutions for documents for third country nationals, EU citizens' passports and information systems (VIS and SIS II). The European Council invited the Commission to prepare the appropriate proposals, starting with visas, while fully respecting the envisaged timetable for the introduction of the Schengen Information System II. Commission's proposal of September 2003 to lay down a uniform format for visas and residence permits for third country nationals is worth particular mention in this respect. The proposals provide for the mandatory storage of the facial image as a primary biometric identifier and the fingerprint as a secondary biometric identifier that should be added. There are also current proposals to introduce the biometric data in the passports of the EU citizens.[2]

Improvements to VIS could contribute to addressing a number of other problems in the current visa issuing situation, including:

- Visa application fraud, visa shopping and travel document fraud;
- Limitations of border checks, based heavily on inspection of travel document presented;
- Illegal migration, including overstaying the period allowed by the border control authorities, following production of the visa;
- Inability to combat internal security problems, including terrorism, and the use of falsified travel documents and visas by terrorists;
- Inefficiencies for bona fide travellers[3] when they lose their passports in the Schengen area. Also, repeat visa applications by bona fide travellers are not facilitated, due to a lack of knowledge about previous visa applications and compliance by the applicant in the past with immigration requirements.

The Council has set a number of objectives for the visa information system in its conclusions of 19 February 2004:

- "constitute an instrument to facilitate the fight against fraud, by improving exchanges of information between the Member States (at consular posts and at border crossing points) on visa applications and responses thereto;
- contribute to the improvement of consular cooperation and to the exchange of information between central consular authorities;

[2] Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports, Brussels, 18.2.2004, COM(2004) 116 final, 2004/0039 (CNS).

[3] The term 'bona fide traveller' is used to refer to third country nationals who travel to the Schengen States on leisure and business purposes, have not nor intend to breach their visa and other immigration requirements, and do not constitute a threat to internal security.

- facilitate checks that the carrier and the holder of the visa are the same person, at external border checkpoints or at immigration or police checkpoints;
- contribute to the prevention of "visa shopping";
- facilitate application of Council Regulation (EC) No 343/2003 determining the State responsible for examining applications for asylum;
- assist in the identification and documentation of undocumented illegals and simplify the administrative procedures for returning citizens of third countries;
- contribute towards improving the administration of the common visa policy and towards internal security and to combating terrorism."

VIS could provide an impetus for consular co-operation and further the implementation of common visa policy. VIS could also be effective in combating visa fraud, visa shopping, travel document fraud and improving external border checks. In addition, VIS would be a contributory instrument in combating illegal migration and improving internal security, including fight against terrorism.

The following policy options were assessed in the study:

- 'No VIS'.
- 'Entry-exit system' similar to the US-VISIT (US-VISIT system is described in detail in Annex 1).
- 'VIS without biometrics'
- 'VIS with biometrics'.

The costs associated with the policy options can be summarised as follows:

	Financial costs	**Opportunity costs for visa applicants**	**Retaliation costs for EU travellers**	**Reductions in business travel and tourism**	**Impact on privacy and human rights**
No VIS	-	-	-	-	-
Entry-exit system (with biometrics)	√√√√	√√√	√	√	√√√
VIS without biometrics	√	-	-	-	√
VIS with biometrics	√√√	√√	√	√	√√√

√√√√ Exorbitant

√√√ Very significant

√√ Medium

√ Small

- No change from present situation

In terms of financial costs, which cover the one-off investment costs and annual operational costs of running a computer-based system like VIS, the highest costs would be associated with the entry-exit system, as it would require all the consular

posts, and entry and exit border points to be properly equipped. 'VIS with biometrics' would carry significant financial costs, compared to the policy option 'VIS without biometrics', due to the inclusion of biometric data in the system.

Because all visa applicants will be required to come to the consular posts to provide their biometric data, opportunity costs (i.e. in terms of time and travel costs) would be high in the 'VIS with biometrics', but highest in the 'Entry-Exit system'. It can also be expected that some third countries would retaliate to the introduction of biometric data in the VIS as a consequence of perceived intrusion into the privacy of their citizens. One measure could be imposition of requirement to provide biometric data when EU citizens apply for a visa to come to these countries, which could carry an opportunity cost for EU citizens.

If biometric data is introduced in the VIS, it could also be expected that some reductions of business and leisure travel would occur, due to the perceived intrusion into the privacy of individuals. The introduction of biometric data in any policy option would have a very significant impact on privacy and fundamental rights of third country nationals, due to the sensitive nature of such data.

The benefits associated with policy options can be summarised as follows:

	Efficiencies in implementation of Common Visa Policy	**Facilitation of Dublin II regulation**	**Reductions in fraud and visa shopping**	**Increased efficiency of border checks**	**Reductions in illegal migration**	**Contri-butions towards internal security**	**Increased efficiencies for bona fide travellers**	**Other spin offs**
No VIS	-	-	√*	√*	√*	√*	-	-
Entry-exit system	√√√	√√√	√√√	√√√	√√√	√√	√√√	√√√
VIS without biometrics	√√	-	√√	√√	√	√	√√	√
VIS with biometrics	√√√	√√√	√√√	√√√	√√	√√	√√√	√√√

√√√ Very significant

√√ Medium

√ Small

√* Impact conditional on the effectiveness of current developments and developments planned (including SIS II)

-No change from present situation

The advantages and drawbacks of the policy options can be summarised as follows:

- 'No VIS' option has a low financial cost, but no improvements in the exchange of visa application information are expected. In addition, document fraud and visa shopping would not be reduced.
- In the 'entry-exit' system, substantial reductions of current problems would occur. However, this policy option carries exorbitant financial costs and high social impacts in terms of intrusion into privacy of travellers.
- 'VIS without biometrics' would carry a moderate financial cost and would bring about some improvements in relation to the problems in the current situation. However, it would not provide a reliable personal identity verification.
- 'VIS with biometrics' would bring substantial improvements in most domains. It would, however, entail high financial costs and substantial social impacts. In this policy option, there will also be no records on persons leaving the territory of Schengen States.

Regarding the proportionality and added value of European action, the following assessments have been made.

	Proportionality	**European added value**
No VIS	Does not address all of the political objectives set and only some improvements in the problems in the current situation could be anticipated	None
Entry-exit system (with biometrics)	Substantial improvement, however, a huge organisation step change from current situation, risky and extremely costly to implement	As for 'VIS with biometrics' but also enables comprehensive immigration controls
VIS without biometrics	Moderate financial costs but addresses the problems in the current situation and political objectives set to a certain degree	Facilitates exchange of information on visas on a regular and comprehensive basis to enable implementation of common visa policy
VIS with biometrics	High costs but would tackle many of the problems identified and meet political objectives set	Facilitates exchange of information on visas on a regular and comprehensive basis to enable implementation of common visa policy Identification of visa applicants with the use of biometrics enables reliable and immediate exchange of information Contributes to an effective return policy

The study assessed in detail the policy option 'VIS without biometrics' and policy option 'VIS with biometrics'. Both policy options would provide access to visa application

information to all Schengen States and would encourage consistency in the visa issuing process.

However, 'VIS without biometrics' would carry a small financial cost, compared with the high financial costs of the 'VIS with biometrics'. The former would also have a lesser social impact and intrusion into privacy of third country nationals than 'VIS with biometrics'. In contrast, the major advantage of 'VIS with biometrics' would be a reliable identification and verification of visa applicants and travellers, whereas in 'VIS without biometrics' there would still be continuing difficulties in this area. Inclusion of biometric data into the VIS would also have a larger impact on reducing fraud and illegal immigration, and make a more substantial contribution to internal security.

VIS with biometrics would make a contribution to the fight against illegal migration as it would allow the identification of undocumented illegal migrants apprehended in the territory of Schengen States and who have applied for a Schengen visa before (if their data would be still held in the system, given the limited retention period). No European statistics are available on the proportion of third country nationals who enter the territory legally with a visa, but then overstay the permitted period of stay. However, VIS with biometrics would also help to identify these people, if they are apprehended.

VIS with biometrics would also make a contribution to internal security including the fight against terrorism, as it would provide a tool to the consular authorities and to the services responsible for carrying out checks at external borders and within the territory of the Member States to better examine visa applications. One of the basic aims of the visa policy is to make sure that persons who are a threat to internal security are not granted a visa to enter the territory of Schengen States. The processing of biometric data in the VIS would ensure exact verification and identification of visa applicants.

VIS will also have an impact on the practice and the standards of consular authorities, and the introduction of procedures of taking biometric data will require changes in the Common Consular Instructions.

In the implementation of VIS (with or without biometric data) data protection considerations will be of paramount importance. In particular, there is a risk of "purpose creep" (i.e. the use of personal data for purposes other than originally envisaged in the VIS) and need to define and enforce tight access rights. Also, third country nationals must have a right of access to their records, and independent data supervisory regime is needed to monitor the effectiveness of data protection. In particular, the principles of proportionality and necessity of the storage and processing will have to be implemented in full. It is also worth noting that these parameters depend on what biometrics are taken, for how long they are stored and what authorities will have access to the data (these questions are explored in greater detail in sections 5.5-5.8 and Annex 3 to this report).

Data protection requirements relevant for the implementation of the VIS are considered in detail in Annex 3.

INTRODUCTION

Background

The rationale for this study is the high priority given to the establishment of a legal framework for the proposed Visa Information Exchange System (VIS), which represents one of the key initiatives aimed at maintaining the area of freedom, security and justice in the EU. Bearing in mind the important implications from a political, social and financial perspective for a wide range of stakeholders, it was decided that this initiative should undergo an extended impact assessment (EIA). The purpose of this study is to support Commission services in elaborating the Extended Impact Assessment.

Accordingly, this study for the EIA has been conducted in view of preparation of the proposal for a fully fledged legal instrument concerning the VIS. The study for the EIA is intended to allow the political decision-makers (initially in the College of Commissioners, then subsequently in the Council and European Parliament) to make a political decision on a proposal, which has been drafted in the light of the evidence analysed and presented in this study for the EIA. The publication of the EIA, along with the proposal, enhances the transparency for stakeholders and EU citizens in general, by allowing them to judge the extent to which the proposal is in line with the evidence presented in the EIA.

This study for the Extended Impact Assessment was conducted by a team from the European Policy Evaluation Consortium (EPEC, www.epec.info). The assignment was undertaken under the guidance of an Inter Service Steering Group.

The aims of the study for the EIA of the VIS are:

- Elaborate the current problems in relation to the issue of visas;
- Assess the fit between political objectives of VIS and these problems;
- Assess the costs and benefits of policy options available to address the identified problems in the current situation.

EPEC's methodological approach to this study for the EIA consisted of several elements:

- Desk research and review of official documents, reports and other studies relevant to visa policy in the EU;
- Consultations with relevant Commission Services;
- A review of the results of consultations with the relevant authorities in the Member States;
- A review of the results of online public consultation launched on the DG JHA website.

The full list of information sources used in the course of the study is provided in the Annex 6.

The team established by EPEC to conduct this study for the EIA has wide experience and included migration and visa experts with experience and close contacts within immigration control authorities, visa issuing agencies, and other relevant agencies in many countries. This experience has been vital in undertaking this study, as there are a number of areas within which no statistical data, source of material or empirical evidence is quoted, but where informed judgments have been necessary.

The study started with the inception meeting with DG JHA on the 28th May 2004 where initial questions for the study were presented and discussed. Based on these discussions, EPEC submitted an interim report on the 8th July 2004. This report was discussed in the Inter Service meeting on the 14th July 2004, and again with DG JHA officials on the 31st August 2004. A separate meeting to discuss the data protection issues was held with the European Commission Data Protection Office on the 8th September 2004. Inputs from Member State experts into the study were sought on the workshop of 27th September 2004. Following these inputs, this final report is submitted.

1 PROBLEMS IN THE CURRENT SITUATION

1.1 Introduction

The Schengen States of the EU have developed a common visa policy, whereby they issue 'uniform short-stay visas' to third country nationals valid for travelling in the whole Schengen area. The harmonised conditions and criteria to issue uniform format visas are laid down in Articles 9-18 of the Schengen Convention and specified in detail in the Common consular instructions.[4]

The origins of the common visa policy lie in the Schengen agreement of 14 June 1985 on the gradual abolition of checks at the commons borders between Benelux countries, Germany and France. The Schengen Convention abolished the checks at internal borders of the signatory States and created a single external frontier, where checks for all the Schengen signatories were to be carried out in accordance with a common set of rules. There are currently 15 participating Member States which apply the Schengen *acquis* (the Schengen agreements and the implementing decisions).[5]

There are currently 134 third countries whose citizens are required to have a visa issued by a Member State to enter the territory of Schengen States.[6] To obtain a Schengen visa, citizens from these third countries are required to submit a completed Schengen visa application form, providing personal details and details of travel arrangements, as well as a travel document to which a visa may be affixed, and documents supporting the purpose and the conditions of the planned visit. As a general rule, the applicants should be called to appear in person in order to explain verbally the reasons for the application, especially when there are doubts concerning the application. However, this requirement is waived in cases where the applicant is well-known or where the distance from the consular post is too great, provided that there is no doubt as to the good faith of the applicant, and, in case of group trips, a reputable and trustworthy body is able to vouch for the good faith of those persons concerned. After verification of the application, a decision is made on the issue of a visa.

Current statistics show that Member States (including Iceland and Norway but excluding the new Member States) receive around 12 million visa requests per year (VIS feasibility study). Based on these figures, it is expected that the number of visa

[4] Common Consular Instructions on visas for the diplomatic missions and consular posts, Volume 46, C 310, 19 December 2003.

[5] Belgium, Denmark, Germany, Greece, Spain, France, Italy, Luxembourg, Netherlands, Austria, Portugal, Finland and Sweden as well as Iceland and Norway. Ireland and the United Kingdom do not participate in the Schengen *acquis* concerning the lifting of internal border controls and the common visa policy and have thus not ended border controls with other EU Member States. In accordance with the Protocol on the position of Denmark, Denmark can choose within the EU framework whether or not to implement any new measure building on the Schengen *acquis* in its national law.

[6] Annex 1, Common Consular Instructions on visas for the diplomatic missions and consular posts, Volume 46, C 310, 19 December 2003.

requests will reach 20 million by 2007, taking into account the new Member States. Some visa issuing figures for some Member States are given in Annex 4.

The main problems that the VIS and other policy options considered in this report should address are:

- Inefficiencies in the implementation of EU policies (Common Visa Policy and Dublin II Regulation determining the state responsible for examining the application for asylum);
- Visa fraud, 'visa shopping' and travel document fraud;
- Inefficiency of border checks;
- Illegal migration (including those overstaying on visa);
- Internal security and terrorism;
- Inefficiencies for bona fide visa holders (including regular travellers and those who lose their travel documents in the Schengen territory).

Each of these problems is elaborated below.

1.2 Inefficiencies in implementation of EU policies

Currently, a third country national can obtain a Schengen visa and travel freely within the territory of Schengen States. However, information about his[7] visa application is routinely held only by the Member State that issued the visa. If a bona fide traveller applies for a Schengen visa again, but to the authorities of another Member State, the record of his past visa application(s) is not readily available to the consular authorities of that other Member State. Also, when a third country national is refused a Schengen visa, the authorities of the Member State which refused his application routinely store the record of the rejection. Apart from a rejection stamp in his passport (which can be easily removed or a new passport obtained), authorities of other Member States do not know about such a refusal, should the same person apply for another Schengen visa to the authorities of another Member State.

There is some important exchange of visa data under current arrangements, for example, through local consular co-operation and VISION (Visa Inquiry Open-border Network) consultation. Local consular co-operation concerns the assessment of immigration risks and is used to exchange information on the use of false of documents, on possible illegal migration routes and on refusing visas where applications are fraudulent. Such exchange is done by regular meetings depending on circumstances and as deemed suitable by consular authorities (as specified in the Annex 5B to the Common Consular Instructions).

VISION is a Schengen consultation network established for the purpose of consultation on visa applications between central authorities of the Member States. The process is initiated by visa issuing authorities for applicants where their country of origin is in the list of sensitive countries (listed in the Common Consular instructions on visas).[8]

[7] In this report, the use of words he/his/him do not carry gender connotation.

[8] The following process is employed: the diplomatic mission to which the visa application has been lodged by one of the categories subject to consultation transmits this application to central authority in its country. This authority disseminates a message for consultation to one or more Member States which have asked to be

VISION is currently a message exchange system, based on the bilateral exchange of information.

It follows that the existing information exchange arrangements are partial, bureaucratic, time consuming and can be inaccurate.[9] Exchange of information between consular posts at many places is carried out by telephone, email or meetings, and through procedures that do not ensure that the information is always readily available in a timely fashion.[10] The risk of transmitting inaccurate or incomplete information in such exchanges will now be greater with 25 Member States (plus Norway and Iceland), whose consular missions will be working at a local level, in different time zones with different opening hours.

There are also issues associated with the implementation of the Dublin II Regulation[11], the aim of which is to determine the member state responsible for the examination of an asylum claim. The Dublin II Regulation states that a Member State, which has issued a visa to travel for a person, is also responsible for dealing with his/her asylum application. The Dublin II Regulation also provides for the possibility for the Member States to request information about a visa issued by another Member State, in order to facilitate the examination of an asylum claim. At the moment, Member States do not have an efficient means to check whether an asylum applicant has had a visa issued by another Member State, verify the identity of the person, and find out how long the visa is/was valid for. All this information is required to identify the Member State responsible for the examination of asylum application.

1.3 Visa application fraud, visa shopping and travel document fraud

1.3.1 Visa application fraud

It is also apparent in the current situation that there is a sizeable proportion of people who try to obtain a Schengen visa on dubious grounds. Visa refusal statistics from Member States are one of the indicators of the extent of this.[12] In Germany, for example, around 15% of all visa applications were rejected or visas refused in 2002.[13] Similarly, 15% of visa applications were unsuccessful in the UK in 2002.[14] Council statistics show that around 25% of visa applications do not lead to visas being issued, either because they are refused or no longer requested. This could be because of a change of travel plans, or because the application is formally withdrawn or otherwise

---

consulted, and the consulted country/countries communicate their response to the central authority of the Member State which requested consultation. For countries, where consultation is not requested by any of the Member States, VISION consultation is not evoked.

[9] In the process of consultation for the EIA, several Member States provided an example of inaccuracy and confusion in consultation where visa applicants have similar names and dates of birth.

[10] This has been confirmed by replies of Member State officials to the questionnaire distributed by DG JHA in connection with this EIA.

[11] Council Regulation establishing the criteria and mechanisms for determining the Member State responsible for examining an application for asylum lodged in one of the Member States by a third-country national. (EC) 343/2003.

[12] Visa refusal statistics do not record in detail the number of refusals where applications were simply incomplete rather than fraudulent or in breach of visa issuance regulations.

[13] New Visa Practice of the Federal Foreign Office, www.auswaertiges-amt.de.

[14] Entry Clearance, Facts and Figures, www.ukvisas.gov.uk.

not pursued, for example because the applicant realises that it would not succeed, or makes other travel plans.

Visas are refused for a variety of reasons - failure to produce the required documentation or necessary supporting evidence (bank statements or sufficient, appropriate sponsorship), or because the applicant's stated intentions and purpose of stay are not credible. Broader exchanges of information about unsuccessful applications made elsewhere, and in particular details of fraudulent applications, would assist visa officers to judge the validity of cases under consideration by them.

At present, Member States have difficulties in ascertaining whether a visa applicant is using a false identity to obtain a Schengen visa. It is relatively easy to change identity by means of a new, counterfeit or falsified passport without it becoming immediately apparent to consular and border checking posts. Information on stolen or false travel documents is not readily available to consular posts and border checking points. Information on dubious references to support visa applications (persons or companies) is also not readily available to consular posts. The existing system for exchanges of information does not ensure that information reaches the missions or border control points that require it on time.

1.3.2 Visa shopping

Currently, after refusal of a Schengen visa by one Member State, the refused person can apply for a visa to another Member State, even within the same country of application, with a high possibility that a previous visa refusal would not be identified. There is no formal information system for authorities to check whether the applicant has applied and been refused, or has failed to pursue a Schengen visa application previously, or indeed whether a visa has been granted to the individual in the past.

Visa shopping occurs following a visa refusal in one Member State, and/or because third country nationals think it may be easier to obtain a Schengen visa from some consular authorities rather than others, bypassing the criteria for the determination of the Member State responsible for examining the visa application. It is worth noting that while the criteria for issuing visas to third country nationals are the same for all Schengen States, there could be a perception that the assessment and application of criteria may differ substantially in the region and country in question. Indeed, it is questionable whether it is feasible to have a uniform interpretation of visa issuing instructions with 12,000 users working in 3,500 consular posts worldwide. Consular officers are taking appropriate decisions on a visa application on the basis of all the information available, bearing in mind the specific situation of each applicant.

1.3.3 Travel document fraud

Statistics from several Member States give an indication of the scale of the travel document fraud. France reported questioning 13,952 persons carrying false documents in 2002, which was a 14% rise compared to 2001.[15] In the UK 7,985 abused travel documents were detected in UK arrival controls in 2003.[16]

[15] The activity of National Police, Ministry of Interior of the Republic of France, 27 January 2004.

[16] Passports – House of Commons Hansard Written Answers for 28 June 2004 (pt 7).

It is well established that serious and organised criminals (and most of the criminal organisations) operate on an international basis. Criminals often have both the finance available and the contacts to enable them to obtain high quality falsified documents. These may be complete counterfeits, documents obtained using false supporting evidence (for example the birth certificate of another person), or a document genuinely issued to another person may have been altered without authority. This may involve substitution of the photograph and/or alteration of personal details, such as the date and place of birth.

When border control or other officials identify documents that have been tampered with, it is frequently found that the original document has been reported stolen by the genuine holder. In addition, burglaries have been carried out at embassies or consulates, in the knowledge that authentic passports are stored there. As a result, batches of genuine, original documents have become available to the criminal fraternity, ready for the photograph and personal details to be entered of the person to whom they were to be sold.

As indicated above, in addition to genuine documents bearing false details, entirely counterfeit passports are used for illegal migration, and other criminal purposes. Skilled forgers may produce extremely convincing copies of passports and other documents of identity, and indeed of other documents needed to obtain them, such as the birth certificate. US immigration officers have given falsified birth certificates the nickname “breeder documents”, as one such document can produce various forms of other identity documents.

A matter of current concern to control authorities is that the power of modern desktop technology - computers, digital photography, scanners and colour laser printers - have made falsification much faster and cheaper.

The main types of travel documents falsified include:

- Passports and other travel documents – the different types of false passports and identity cards detected include those that are entirely counterfeit, those that have been altered (perhaps by the replacement of the photograph), and those that are used which belong to another person with similar features - in other words by impersonation. This misuse of genuine travel documents by imposters is understood to be widely exploited by nationals of some countries. Cases have been reported where third country nationals have used a document apparently issued genuinely to him by a country of which he speaks the language, for example a Spanish document, in the case of nationals of certain South American countries, or a Portuguese one, in the case of Brazilian, Angolan or Mozambique nationals.
- Visas - counterfeit visas are produced, and genuinely issued visas are altered, to match as closely as possible the personal particulars of the fraudulent holder. Visas may also be transferred unlawfully from the document in which they were endorsed to another one and visa refusal endorsements may be removed without authority. There are also cases where visas are obtained by false representations, for example by a person claiming to be a visitor or student, when the real intention is to remain for employment or other long-term purposes.

- The misuse of genuine travel documents by imposters, the so-called “look-a-likes” is also exploited, particularly amongst some nationalities.

1.4 Limitations of border checks

Officers at border checkpoints at the external EU borders assess whether third country nationals have fulfilled the applicable entry conditions. They conduct visa and traveller verification for travellers from third countries. Existing border checks are based on the examination of the holder of the document, of the document itself, and of any visa contained. This includes both visual inspection and the use of document examination and forgery detection equipment. Furthermore, the Schengen Information System (SIS) is consulted in order to ascertain whether an alert has been issued for the purpose of identifying a third country national, with a view to refusal of entry, if appropriate.

In making such checks, border control officers rely heavily on the passport shown to them. Visa sticker authenticity is determined by examining its security features. To make visa stickers less prone to fraud, existing arrangements require the integration of the photograph with the visa sticker. Proposals are also underway to integrate biometric data into the visas and residence permits for third country nationals.

If there is a need to check in another Member State whether the visa a person carries in his passport was given to the holder of the passport or whether it has been transposed from another passport; this is possible, but it is a time consuming procedure. Border control authorities can check the authenticity and validity of a visa with the authority that issued the visa, but such activity requires time and it may be difficult to obtain the information quickly.

One difficulty experienced by those authorities in Member States seeking to exchange information is that their counterparts in other countries may be from a different control authority to that responsible in their own State. The Police tend to be responsible for the control of persons, and Customs are responsible for goods. However, in a number of States more complicated structures exist, and exchanges of information would be facilitated by an information exchange system with well-established criteria about information that merits dissemination, and proper procedures as to its circulation.

Border checks would be greatly facilitated in the case of visas, if the border control officer had easy access to accurate information about the person based, for example, on biometric identification. This would decrease the possibility that a person travel could with the visa issued for someone else, in order to conceal his/her true identity.

Member State governments are realising that procedures at external borders need to be tightened. Immigration officers at the front line - airports, ports and border checkpoints - need to be well equipped in order to tackle passport and visa fraud. Ideally, every booth at a point of entry should be equipped with a computer linked to a database. It then takes immigration officers only a few seconds to access details of wanted suspects and others who should not be admitted, and details of falsified and stolen passports may be stored. They should also have the necessary tools to ascertain that a document is genuine and has not been altered (e.g. infra-red and ultra-violet lamps) and read the data stored on the machine-readable zones of any travel documents they need to check. Border guards need training and tools to help them

recognise false documents such as passports, as well as a continuous system to inform other countries when they find false documents.

1.5 Illegal migration

The very nature of the problem makes it impossible to say how many illegal migrants enter or remain in the EU.[17] The current evidence suggests annual inflows of illegal migration into the EU reaching over six figures, although any indications of numbers should be treated with extreme caution.[18] In some countries large-scale regularisations of illegal migrants can provide a certain estimation of the numbers involved.[19]

However, it is well established that illegal migration is a major concern to governments world-wide, and this has been recognised within the EU, in a range of policy and legal instruments, for example the Communication on Common Policy on Illegal Migration,[20] the EC Green Paper on a Community Return Policy on Illegal Residents[21], the EC Communication on a Community Return Policy on Illegal Residents[22], and the EU Return Programme[23].

In 2001, around 360,000 people illegally present in the EU territory were apprehended. In the same year, around 390,000 people illegally present in the EU territory were removed and around 1.2 million non-EU citizens were refused entry. [24]

Illegal migration takes a number of different forms:

- A person enters without lawful authority, for example, clandestinely, hidden in a lorry, other vehicle or container, or across an unsupervised border;
- Some people enter through a border post, but do so using a counterfeit or falsified travel document or visa. This may often be of high quality and be provided as part of the package arranged by the person or organisation facilitating the illegal entry;
- Alternatively, immigrants might have valid travel documents, but produce false supporting documents, for example, regarding financial background, or

[17] A pilot scheme involving coordinated border checks at 25 European airports during one month in 2002 resulted in the detention of nearly 5,000 illegal immigrants, the seizure of nearly 1,000 false travel documents and the arrest of 34 human traffickers. The scheme also showed that most people who enter the EU illegally arrive not by sea, but by air at major European airports, often posing as tourists. The largest group comes from China, followed by Ecuador and Angola, and the main arrival points are Paris, Madrid, Milan, Dublin and London.

[18] Study on the links between legal and illegal migration, COM(2004) 412 final, 4 June 2004, p. 11.

[19] In Italy around 217,00 undocumented foreigners were regularised in 1998, quoted in A Common Policy on Illegal Immigration, Select Committee on the European Union of the House of Lords, Session 2001-02, 37th Report, p. 12.

[20] COM(2001) 672 final , 15 November 2001.

[21] COM(2002)175 final, 10 April 2002.

[22] COM(2002) 564 final, 14 October 2002.

[23] Proposal for a Return Action Programme, The Council of the European Union, 14673/02, MIGR 125, FRONT 135, VISA 172, 25 November 2002.

[24] Annual Report on Asylum and Migration, European Commission, 2001. The figures refer to the EU25.

make other false statements in order to obtain a visa or permission to enter at the border;

- Immigrants also travel to a third country with their own genuine documents, which are then destroyed and immigrants are supplied with a falsified or stolen passport from a country that has no visa requirement for the desired final destination country in the EU;[25]
- A person who has previously been refused a visa may obtain a new, genuine passport, in his own identity, claiming to his national authorities that the previous document was lost or stolen. He may then re-apply, at a different visa issuing post, possibly to another Member State's consular authorities. In the absence of well-organised exchanges of information between the consular posts concerned, it is quite possible that the previous application will not be identified;
- Similarly, a person refused a visa may obtain a new passport in another identity, by producing fraudulently obtained supporting documents. Alternatively, he (or someone acting on his behalf)) may be able skilfully to remove, or have removed, any stamp recording the refusal. A visa may then be obtained by concealment of the material facts relating to the previous application, and thus unlawfully.

Equally, there are cases in which people who have entered lawfully overstay or breach the conditions of their stay by entering employment without obtaining permission from the relevant authorities.[26] It is difficult to estimate the scale of this phenomenon in the territory of Schengen states, as most European countries do not keep statistics of overstayers on visas. Where such statistics do exist, they show that overstayers outnumber other categories of illegal migrants.[27]

Many of the apprehended illegal migrants have no travel or other identification documents with them or use counterfeit or falsified documentation.[28] In such cases, the identification process is slow, time consuming and expensive. Many of these people enter Schengen after having applied for a Schengen visa but having the application turned down, or enter the Schengen area holding a visa but having destroyed or hidden his/her documents after entry. In these cases, the authorities have no readily available system to check the identities of the undocumented illegal migrants.

The determination with which illegal migration is being tackled within the EU indicates a clear recognition that illegal migration is against the public interest. It is also well recognised internationally that people who enter or remain illegally are frequently the victims of human traffickers or smugglers.[29] This may not only be because of

[25] Organised illegal immigration into the European Union, January 2004, Europol, p. 4.

[26] Study on the links between legal and illegal migration, COM(2004) 412 final, 4 June 2004, p. 10.

[27] Australia reported 58,748 overstayers in 2000, compared to 1695 arriving unauthorised by air and 4,175 arriving unauthorised by sea, quoted in A Common Policy on Illegal Immigration, Select Committee on the European Union of the House of Lords, Session 2001-02, 37th Report, p. 11.

[28] Organised illegal immigration into the European Union, January 2004, Europol, p. 4. in the course of the consultations on the EIA, one Member State estimated that 90% of illegal migrants arrive without any official documents.

[29] Trafficking of human beings: a Europol perspective, January 2004, p. 3.

payments initially extracted from them, but also through continuing commitments to those who have facilitated their illegal entry of stay. It follows that steps taken to minimise illegal migration are in the public interest, and may also be viewed as reducing the risk of vulnerable people becoming prey to those prepared to profit from them.

1.6 Internal security and terrorism

The inefficiencies in combating visa shopping, fraud and of conducting the border checks are also causing inefficiencies in relation to internal security of the Member States. Typically, terrorists do not travel under their own identity, or alters his personal details, such as his date of birth, to make identification more difficult. In particular, this may be so if the person has been 'flagged up' with those responsible for visa issuing, border controls, or after-entry enforcement being involved in terrorist and other criminal activities. He will be very aware of the reliance placed by control authorities on intelligence and other information about those involved in terrorist activity. He may also have substantial financial backing to allow skilful, unauthorised alterations to be made to his travel documents or indeed to obtain high quality counterfeits.[30]

If the identity is changed, or if material alterations are made, any adverse history may be very difficult to identify. Similarly, any intelligence gathered about the individual will be nullified. The attraction to the terrorist or potential terrorist of other criminals of changing his identity or personal details, as shown in his travel document, under present arrangements, is apparent. However, if checks are also made of biometric data, retained at the time of a previous visa application, the true identity should be revealed.

Of course, terrorists and potential terrorists may be aided by officials in some third countries, prepared to give those with whom they sympathise (or by whom they have been bribed) a travel document in a false identity, and to replace this with other documents when the need arises. In such circumstances, a simple identity check, for example on name, nationality and date of birth, is likely to give no positive match. As with illegal migrants, it may still be possible for a terrorist to enter clandestinely, or with a skilfully falsified travel document, showing a nationality, for which no visa is required.

Organised criminals may be aware that details of their name, date of birth, nationality and crimes(s) committed will be maintained by enforcement agencies, stored on a "warnings" system such as the SIS, and in appropriate cases passed to visa issuing authorities. They may counter this by obtaining a travel document in another identity, or by altering material personal particulars.

Like many involved in terrorism they may have substantial means and organisational structures to make skilful alterations to travel documents, or indeed to manufacture high quality counterfeits.

So it is apparent that terrorists and organised criminals do use false visas or documents belonging to other persons to enter the EU without being detected. The absence of biometric identifiers means that terrorists may not have to use documents

[30] Indeed, the 9/11 Commission in the United States noted that 'for terrorists travel documents are as important as weapons … [and] terrorists use evasive methods such as altered and counterfeit passports and visas, specific travel methods and routes …', p. 384.

properly issued to them, and it is relatively easy to change identities. Hence, they have more possibilities to come into the EU without being identified by the authorities.

1.7 Impacts on bona fide visa holders

In cases of lost or stolen travel documents bona fide travellers have to go through a complicated and protracted process to establish their identities in order to acquire new travel documents.[31] There is also a high risk inherent in this situation with such stolen travel documents and visas used to enter the territory of Schengen States – the original holder may need to re-apply, if he has not yet used the visa, and the document holding the visa may be used by a person not entitled to it. The absence of comprehensive data to check the identity of visa holder and actual traveller increases the possibility of fraud in this respect.

Of all travellers applying for a Schengen visa, 20% are estimated to be regular travellers, i.e. applying for a visa several times. For regular travellers there is currently little scope for speeding up the visa processing times which would take into account the fact that such travellers have complied to the visa and immigration requirements in the past. It is also worth mentioning that regular travellers are usually business travellers, for whom such facilitation of their visa applications would aid the conducting their business activities in the EU.

[31] The term 'bona fide traveller' is used to refer to third country nationals who travel to the Schengen States on leisure and business purposes, have not nor intend to breach their visa and other immigration requirements, and do not constitute a threat to internal security.

2 POLITICAL OBJECTIVES AND ORIENTATION SET BY COUNCIL

As stated in the Council conclusions of 19 February 2004,[32] "the Visa Information System (VIS) is a system for the exchange of visa data between Member States, which must meet the following objectives:

- constitute an instrument to facilitate the fight against fraud, by improving exchanges of information between the Member States (at consular posts and at border crossing points) on visa applications and responses thereto;
- contribute to the improvement of consular cooperation and to the exchange of information between central consular authorities;
- facilitate checks that the carrier and the holder of the visa are the same person, at external border checkpoints or at immigration or police checkpoints;
- contribute to the prevention of "visa shopping";
- facilitate application of Council Regulation (EC) No 343/2003 determining the State responsible for examining applications for asylum;
- assist in the identification and documentation of undocumented illegals and simplify the administrative procedures for returning citizens of third countries;
- contribute towards improving the administration of the common visa policy and towards internal security and to combating terrorism."

There is a close correspondence between the specific objectives of VIS and the problems identified and elaborated in Section 1 of this report. The VIS is primarily intended to improve the implementation of the common visa policy, including the use of visa data for the objectives set out in the Council conclusions.

[32] Council Conclusions on the development of the VIS of 19 February 2004 (6535/04).

3 POLICY OPTIONS AVAILABLE TO REACH POLITICAL OBJECTIVES

3.1 Introduction

This section describes four policy options that are assessed in the Extended impact Assessment. They are:

- Policy option 1 'No VIS';
- Policy option 2 'Entry-exit system (with biometrics)';
- Policy option 3 VIS without biometrics;
- Policy option 4 VIS with biometrics.

3.2 Policy Option 1 'No VIS'

The 'No VIS' option should not be considered as a 'do nothing' scenario. Rather it should be viewed as a situation where the VIS (with or without biometrics) would not be established, but other developments go ahead, which have potential to contribute towards political objectives. If the VIS is not created, the following developments in the current situation, which have potential to meet the political objectives, may be noted:

- Implementation of Common EU Visa Policy will continue, including such recent developments as making visas more secure and difficult to counterfeit by including biometric data in visa stickers;[33] exchanges of information on visa issuing trends at local consular level; and establishment of liaison officers at immigration hot spots. However, it is worth noting that the counterfeiting of travel documents is also becoming more and more sophisticated and technologically advanced, in parallel with the developments to increase the document security.
- Continuing use of VISION, which is a network to support current co-operation of central authorities. The process is initiated by visa issuing authorities for visa applicants where their country of origin is in the list of sensitive countries. VISION is a system of primarily *bilateral* exchanges of information between Member States. The VISION consultation network relies on outdated messaging exchanges technologies. If a decision for the creation of the VIS is made, the Council in the conclusions of 19 February 2004 recommended integration of the technical functionalities of the VISION into the VIS.

[33] Commission's proposal of September 2003 to lay down a uniform format for visas and residence permits for third country nationals is worth particular mention in this respect. The intention in the proposal is to bring forward the final date for the implementation of photograph in visas and residence permits from 2007 to 2005 and at the same time, and to require Member States to integrate biometric identifiers into the visa and the residence permit for third country nationals in a harmonise way. The proposals provide for the mandatory storage of the facial image as a primary biometric identifier and the fingerprint as a secondary biometric identifier that should be added. See Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas and a Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third country nationals, COM(2003)558 final, 24 September 2003.

However, it is also worth noting that the nature of VISION consultation process differs substantially from the comprehensive system of visa information exchange system in that VISION consultation is limited to the third country nationals from sensitive countries and it is a process of bilateral exchange of information.

- Development of the Schengen Information System II (SIS II). By its nature, the Schengen Information System is different from a visa information exchange system:

  – In SIS I, one of the data categories collected is information on third country nationals to be refused entry into the Schengen territory on national security, including public order or immigration grounds (Article 96 check). The SIS I can be consulted by police, border police, customs and partially by authorities responsible for issuing visas via their national SIRENE bureaux. It enables its users to check persons and objects both at external borders and within the territory of the Schengen States.

  – Current developments towards SIS II take into account the need to establish a system allowing the integration of new Member States (SIS I has capacity to deal with 18 participating states). The list of SIS II functions includes the existing functions (such as Article 96 check) and the potential new functions.[34] One new functionality agreed is the ability of authorities responsible for issuing visas to access and search data on EU stolen blank official documents, and identity papers which have been lost, stolen or misappropriated after issue.[35] Other developments include the addition of new alerts, the inter-linking of alerts and the non-mandatory use of biometric information (photographs and fingerprints).[36]

In other words, SIS is not intended to be a system for the exchange of data on visa applications between Member States. It is intended, however, to be a compensatory measure for the removal of internal borders within the EU. It enables police forces from the Schengen countries to access data on specific individuals (i.e. criminals wanted for arrest or extradition, missing persons, and third-country nationals to be refused entry) and goods which have been lost or stolen, as well as to be able to respond to security threats.

- Continuing use of Eurodac database, which was introduced to implement the Dublin II Regulation determining the Member State responsible for examining the application for asylum. The Eurodac fingerprint database, which has been in operation since 15 January 2003, stores the fingerprints of all persons over the age of 14 who have lodged an asylum application in the EU (except Denmark), Norway and Iceland. It allows for the comparison of these fingerprints and helps to determine the Member State responsible for the examination of an asylum application (according to the Dublin II Regulation)

[34] SIS II functions, Council Conclusions of 14 June 2004, 10125/04; Council Conclusions of 5-6 June 2003 on the functions of SIS and the SIS II architecture.

[35] Articles 4 and 5, Council Regulation 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 162, 30.4. 2004.

[36] SIS II functions, Council Conclusions of 14 June 2004, 10125/04.

by establishing whether the individual has already applied for asylum in another Member State or crossed its borders illegally. In addition to fingerprints, the database contains information on the individual's country of origin, the place and date of the asylum application if applicable, their gender and a reference number.

Eurodac aims to prevent multiple asylum applications by the same person by using biometric data to establish whether the individual has already applied for asylum in another Member State or crossed its borders illegally.

3.3 Policy option 2 'Entry-exit system'

The main aims of an 'entry-exit system' are to enable people arriving and departing to be examined, and for appropriate information to be gathered, which is relevant to their immigration and residence status. As such, it may be supported by the requirement for a visa in prescribed circumstances and it would link with after-entry record systems. In relation to foreign nationals, such systems would enable records to be maintained of permission(s) to enter, grants of residence permits, and action for overstaying. It may contribute to improved border checks, more efficient and effective immigration controls, in the broader sense, and increased security, without collection, storage and use of biometric data. In an entry-exit system the identity of all third country nationals will be checked, but biometric data will be required only from visa nationals.

One of the examples of entry-exit system is the US VISIT system, which is envisaged as a continuum of security measures, making full use of biometrics. When a traveller applies for a visa, his fingerprints are taken at the consular post. When the visitor comes to the country, the biometric data are used to verify that the person at the entry point is the same person who received the visa, or to see whether there is new information about any involvement in terrorism or crime. Foreign visitors exiting the country will be required to confirm their departure at the exit points (this is currently at pilot stage at several selected US exit points). This should demonstrate their compliance with immigration requirements and facilitate their future travels. People who overstay their visas would also be identified in this part of the system.

Policy option 2 is thus envisaged as the development of an entry-exit system with biometrics. The study for the EIA will assess the costs and benefits, taking into account the inclusion of biometric data into the entry-exit system. In principle, entry-exit system would be a computerised system for collecting personal details of all visa holders entering and exiting the Schengen territory. Such collection could be done by 'swiping' passport and visa (where these documents are in a machine-readable format), or by keyboard entries in other cases. Such an entry-exit system could also be linked to SIS to enable checks between the two databases by the same 'swiping'/data entry action. The records established on the database would be available to border guards and consular posts issuing visas.

3.4 Policy option 3 'VIS without biometrics'

Visa Information System without biometrics would be an electronic system containing information about the visa applicant from the visa application form as well as decisions taken thereto (including type of visa, status of visa, the competent authority that issued the visa as well as the competent authority that formally refused, annulled, revoked or extended the visa, standard grounds for refusing, cancelling, withdrawing and extending visa, information required for VISION consultation and the results of

consultation, records of person issuing invitation for the applicant, photograph of applicant).

Access to enter and update visa data would be granted to persons authorised to be involved in the visa issuing process or in the process to annul, revoke and extend visas. These authorities would also have access for the purposes of consultation. Provided that visa data is required for the performance of their tasks, other authorities with responsibility for controlling border checkpoints as well as authorities authorised by each Member State, would also have access for consultation purposes.

3.5 Policy option 4 'VIS with biometrics'

Visa Information System with biometrics would contain all the information envisaged in 'VIS without biometrics' (including type of visa, status of visa, the competent authority that issued the visa as well as the competent authority that formally refused, annulled, revoked or extended the visa, standard grounds for refusing, cancelling, withdrawing and extending visa, information required for VISION consultation and the results of consultation, records of person issuing invitation for the applicant, photograph of applicant).

Crucially, 'VIS with biometrics' would also include biometric information of visa applicants (such as fingerprints and/or a digitised image to facilitate facial recognition). All visa applicants would need to visit in person visa issuing posts, or some other authorised point, to provide biometric data.

Access to enter and update visa data would be granted to persons authorised to be involved in the visa issuing process or in the process to annul, revoke and extend visas. These authorities would also have access for the purposes of consultation. Provided that visa data is required for the performance of their tasks, other authorities with responsibility for controlling border checkpoints as well as authorities authorised by each Member State, would also have access for consultation purposes.

3.6 Developments relevant to all policy options

Other developments that have a potential to meet the current political objectives could occur. Amongst such possibilities, the following are noted.

A pilot project to develop Common EU Visa Application Centres has started recently and the first results are expected in early 2005. In this pilot, Member States can use existing co-operation networks and create common visa application centres in third countries. In other words, applications for Schengen visas would be made to this one centre, rather than to national consular offices.

Should the idea of common visa application centres prove feasible and beneficial, the following scenario can be envisaged. In some third countries, one large common visa application centre might operate, and in other third countries the current situation in visa issuing would continue, depending on the local circumstances and setting. There would be substantial limits to the extent to which common visa posts could operate in many of the countries attracting the greatest number of visa applications.

If one considers the countries where the largest numbers of visas are issued, it would be unlikely to be feasible to handle all visas from one post, as the logistics of locating

enough staff together, and of having queuing/interviewing space would be considerable.

This is further apparent when one considers the possibility of Common EU Visa Application Centres developing over the next 5-10 years, and possible merger of relevant tasks in the consular posts of EU25 (plus Iceland and Norway) into one post issuing visas in a third country. One must also take into account the possibility of Common EU Visa Issuing Centres developing over the next 5-10 years.[37] This could happen by merging the consular posts of EU25 (plus Iceland and Norway) into one post issuing visas in a third country and pooling of human resources, though again the difficulties of achieving this in countries handling large numbers of applications are apparent.

It must also be considered that the future SIS II may contain biometric information.[38]

[37] This would be an extension of the idea of common visa application centres.

[38] Articles 4 and 5, Council Regulation 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 162, 30.4. 2004.

4 IMPACT ASSESSMENT OF POLICY OPTIONS

4.1 Introduction

This section of the report considers the relative merits of the four policy options identified in Section 3. Both costs and benefits are considered.

Each policy option is assessed below relative to the following types of costs:

- The direct financial costs to the EU and Member States – over and above those already incurred or anticipated under current arrangements or planned developments;
- The opportunity costs for visa applicants, both financial and other, in terms of travel time and expenses, to apply for and obtain a visa to enter the territory of Schengen States. In considering opportunity costs, account is taken only of anticipated changes in these, if the option under consideration were adopted. This recognises the fact that some such costs may exist under the present arrangements;
- The 'retaliation' costs if the introduction of the policy options should lead to third countries imposing restriction or additional requirements and costs on EU travellers wishing to visit the countries in question;
- Reductions in business travel and tourism to the EU should the policy option deter visitors;
- The 'costs' of the policy options in terms of their impacts on privacy and human rights, through the retention of information and access to that information being extended as a result of the policy options.

Each policy option has been assessed in terms of the benefits that it will bring, relative to the problems outlined in Section 1 and the Council policy objectives described in Section 2. The benefits considered are:

- Efficiencies in implementation of common visa policy;
- Facilitation of Dublin II Regulation;
- Reductions in fraud and visa shopping;
- Increased efficiency of border checks;
- Reductions in illegal migration;
- Contributions towards internal security of the Member States including the fight against terrorism;
- Increased efficiencies for bona-fide travellers;
- Other spin off benefits including the impacts on the EU IT industry.

4.2 Policy Option 1 'No VIS'

4.2.1 Benefits of Policy Option 1 'No VIS'

- *'Efficiencies in implementation of common visa policy'.* The 'No VIS' option would not improve the current lack of information exchange about visa applications. If a visa information exchange system is not introduced, the current situation will continue, meaning that information about visa application of a third country national will be routinely held only by the Member State which issued the visa. Such information would not be readily available to authorities of other Member States when a third country national makes subsequent visa applications to the authorities of another Member State.
- *'Facilitation of implementation of Dublin II regulation'.* The 'No VIS' option would not improve the current situation where Member States do not have efficient means to check whether an asylum applicant has had a visa issued by another Member State, verify the identity of the person, and find out how long the validity of the visa is/was. All this information is required to identify the Member State responsible for the examination of asylum application.
- *'Reductions in fraud and visa shopping'.* Some document fraud reductions are anticipated through envisaged new functions in SIS II and improved security of visas. There has been an introduction of a harmonised system of security features for EU visa and residence documents, intended to help protect against forgery and counterfeiting (e.g. the incorporation of a photograph in the visa).[39] There also has been a substantial effort to boost the levels of equipment, skills and training at document issuing centres and points of entry into the EU.[40] However, these developments to increase visa security[41] are counteracted by increasing sophistication of forgery and counterfeiting techniques. The degree of expertise demonstrated by those fraudulently manufacturing counterfeit travel documents, and making unauthorised alterations to travel documents has increased, and is now aided by the use of technology, including computers, digital cameras and sophisticated colour copiers. The costs of such equipment have fallen in recent years. One can expect yet further enhancements in the degrees of sophistication practised by forgers, and despite exchanges of information and mutual assistance on document examination techniques, it is likely that there will continue to be many cases in which falsified documents are not identified.

---

[39] A European image archiving system called FADO (false and authentic documents) will also be developed to exchange information on genuine and false documents.

[40] For example, Recommendation 1998/C 189/02 detailed the steps EU Member State Governments should take to ensure uniform levels of forgery detection equipment at points of entry into the EU. It cited three levels of provision (minimum, intermediate and upper) based on the qualifications of staff, the quality of the equipment required and the reference documents available.

Recommendation 1999/C 140/01 dealt with the equipment provided to detect falsified documents within the visa departments of representations abroad and in the offices of domestic authorities dealing with visas. Depending on the number of visa applications and the scale of the problems encountered, the Council recommended certain technologies, increased staffing and the training of staff in the new techniques.

[41] Amongst such security enhancing measures is also the proposal to introduce biometric identifiers into the visas, see Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas, COM(2003)558 final, 24 September 2003.

- *'Increased efficiency of border checks'.* Some improvements in efficiency of border checks are anticipated with the introduction of new functions in the SIS II (especially biometric data). SIS II will allow for the integration of the new Member States and update the technology used in the system. The decisions on new functionalities are under discussion at the moment,[42] and some improvements in the efficiency of border checks are expected.
- *'Reductions in illegal migration'.* Some reductions in illegal migration can be anticipated through implementation of existing measures and plans at the EU level. Some measures to tackle illegal migration (as far as a visa policy is concerned) have already been implemented. Amongst them are the introduction of secure visas and exchanges of information on visa-issuing practices; the appointment of Liaison Officers, to be based in immigration "hot spots"; closer liaison with carriers; and the introduction of high-standard external borders control points. However, the fight against illegal migration requires a broader approach. A broad set of measures was developed in the Laeken, Seville and Thessaloniki Councils, which called for better management of external borders, better institutional co-ordination and co-operation, effective return policy of illegal migrants, strengthening of penal code to punish human trafficking, and co-operation with third countries on the management of migration flows.[43]
- *'Contributions towards internal security of the Member States including the fight against terrorism'.* Existing instruments and processes (e.g. national security agencies, Europol, Interpol) can be expected to continue to improve internal security and reduce terrorism. The primary objective of internal security policy is to identify and tackle potential threats to public security. Established intelligence networks which gather, evaluate and disseminate relevant information are the most important tools to deal with the threat of terrorism and organised crime.
- *'Increased efficiencies for bona-fide travellers'.* No increase in efficiencies for bona fide travellers. In the case of travellers who have lost passports, the current procedure of verifying their identity and obtaining new travel documents would remain the same. For regular travellers there will no change in facilitating the issuing of subsequent or multiple-entry visas.
- *'Other spin off benefits including the impacts on the EU IT industry.'* No such additional impacts are anticipated.

If in the long term common EU visa application centres[44] are introduced, this would have the following benefits:

---

[42] One of new functionalities introduced in Regulation 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism is access to data concerning documents relating to persons entered in Accordance with Article 100 (3) (d) (stolen blank official documents) and (e) (issued identity papers that have been stolen, lost or misappropriated) by the authorities responsible for issuing visas and examining visa applications.

[43] For latest overview of measures to combat illegal migration, see Communication From The Commission On The Development Of A Common Policy On Illegal Immigration, Smuggling And Trafficking Of Human Beings, External Borders And The Return Of Illegal Residents. Brussels, 3.6.2003, COM(2003) 323 final.

[44] As noted elsewhere, Common EU Application Centres would not be feasible in countries in which there were large numbers of applicants.

- Reduction in visa shopping would occur because there would be only one visa application and processing point in a third country. The issue of a Schengen visa would remain a decision of national consular authorities, based on the interpretation of common criteria as set out in the Common Consular Instructions. However, national consular authorities would have access to all the past visa applications of a visa applicant.
- Reductions in costs by merging the relevant tasks of the consular posts of 27 participating Member States into one visa issuing centre in a third country and pooling of human and other resources in that way.
- The existence of one central access terminal would make it easier to meet data protection requirements and ensure the security and protection of personal data. There would be one access terminal with practically enforceable access and consultation procedures and clearly defined and limited functions of use.
- Improvements in the implementation of Common Visa Policy. It can also be expected that in 2015-2020 there could be some common EU consulates or at least visa issuing centres. Currently, the EU Member States do issue uniform short stay visas, valid for travelling in the whole Schengen area. The EU has also laid out harmonised conditions and criteria to issue uniform visas. However, the practice and interpretation of the rules is different across the Member States, as demonstrated by the visa shopping phenomenon. The introduction of Common EU Visa Application Centres would be a logical development of the Common Visa Policy. However, as already noted, it would not be feasible to have common application centres in countries dealing with the largest numbers of applications.

4.2.2 Costs of Policy Option 1 'No VIS'

- '*Financial costs'*. Low cost and no additional financial costs apart from funds already committed to the development of SIS II and Eurodac are anticipated.
- '*Opportunity costs'*. No opportunity costs for visa applicants are expected as no change in the current situation is anticipated are anticipated.
- *'Retaliation costs'*. No retaliation costs for EU travellers are expected, as there would be no changes against which third countries might wish to retaliate.
- '*Reductions in business travel and tourism'*. No reductions in business and leisure travel are anticipated, as there would be no change to the current situation in visa application process.
- '*Impact on privacy and human rights'*. No impact on privacy and human rights of travellers is expected, as there would be no change to the current situation in visa application process.

4.3 Policy Option 2 'Entry-exit system'

4.3.1 Benefits of Policy Option 2 'Entry-exit system'

The implications of an 'Entry-exit system', *under which biometric information would be gathered, at visa application stage and at entry and exit points,* are major, and are considered to be as follows.

- *'Efficiencies in implementation of common visa policy.* Although an entry-exit system would provide a continuum of measures to monitor the movements of third country nationals from their application for an entry visa to the arrival at the external border and departure from a territory, the implementation of such a system would go far beyond the objective of improving the implementation of Common Visa Policy through better exchange of information between Member States and indeed other objectives set by the Council for a VIS.
- *'Facilitation of implementation of Dublin II regulation'.* The 'Entry-exit' option would bring substantial improvements to the current situation where Member States do not have efficient means to check whether an asylum applicant has had a visa issued by another Member State, verify the identity of the person, and find out how long the validity of the visa is/was. All this information is required to identify the Member State responsible for the examination of asylum application. In entry-exit system with biometric information gathered at visa application stage and at entry and exit points, the biometric information would provide authorities with means to identify an asylum seeker, if he has been issued a Schengen visa in the past.
- *'Reductions in fraud and visa shopping'.* Considerable reductions in visa fraud (and some reduction in other document fraud) could be anticipated. The introduction of biometric data would provide a reliable base to establish the identity of a visa applicant. It would help to establish a link between the visa holder and the traveller, and reduce the possibility of imposters travelling with visas issued to other people. Considerable reductions in visa shopping could be anticipated. Records of previous visa applications would be readily available to consular authorities when a person applies subsequently for a visa. The inclusion of biometric data would provide a reliable basis to confirm the identity of visa applicant, and reduce the possibility for visa applicants to conceal their previous visa application history (such as a rejected visa or removal from the territory of Schengen States).
- *Increased efficiency of border checks'.* Highly efficient border checks allowing a "beginning to end" survey of movements. The entry-exit system would provide a continuum of measures to monitor the movements of third country nationals from their application for an entry visa to the arrival at the external border and departure from a territory. Such a system would allow the confirmation that the person who was issued a visa is also the same person who enters and leaves the territory of the state. The entry-exit system would also enable more efficient after-entry immigration controls, including enforcement of the immigration laws. It would be possible to check, when a foreign national was leaving the territory, whether he complied with the immigration requirements, and this information would be available when a visa was subsequently sought, and/or on subsequent arrivals. The inclusion of biometric data would provide a reliable basis for establishing the identity of third country nationals throughout the process. Even if an entry-exit system without biometrics is introduced, it could still have beneficial effects in terms of efficiency and effectiveness of immigration control and asylum systems
- *'Reductions in illegal migration'.* Efficient immigration checks would lead to reductions in illegal migration. Undocumented illegal migrants apprehended in the territory would be identified quicker and more efficiently through the entry-exit system in cases when they have applied for a visa in the past. An entry-exit system would also assist in the identification of third country

nationals who overstay the period of permitted stay, since there would be automated records, including details of dates of entry and exit into and from the territory of the Member States.

- *'Contributions towards internal security of the Member States including the fight against terrorism'.* Biometric information would allow the identification and tracking the movements of organised criminals and terrorists, even if they use other identities to apply for subsequent visas or to cross external EU borders. This impact would, however, occur only if terrorists and organised criminals are known as such. In addition, the effects would be limited and dependant on the effectiveness of instruments in Policy option 1 No VIS because:

  – Terrorists may obtain visas and enter, in a false identity, with "genuine" documents supplied by states prepared to assist them;

  – They (and criminals) may enter clandestinely or with a skilled falsification of a passport for which no visa is required; and

  – The ability to identify them is dependent upon prior information about them (biometric or otherwise) being available to the relevant authorities.

- *'Increased efficiencies for bona-fide travellers'.* Increased advantages for bona fide travellers are likely as such a system would establish the past visa and immigration history of a traveller, and demonstrate whether he complied with visa, entry and after-entry requirements in the past. This would lead to the simplification of the repeat visa applications for regular visitors. This would be offset, however, by the inconvenience suffered by bona-fide applicants having to provide biometric data, and submit to close examination at border-checkpoints. In the case of lost or stolen travel documents, biometric information would help to identify the traveller more quickly and facilitate the issue of new documents.

- *'Other spin off benefits including the impacts on the EU IT industry.'* The entry-exit system would provide a big stimulus for IT industries, as it would require the installation and running of state-of-art equipment to capture biometrics and perform checks of travellers in all consular authorities, and entry and exit points in the territory of Member States. The cost estimates for US VISIT system are in the region of $15 billion. However, as US companies dominate the biometrics industry, it is not necessarily the European IT industry that would benefit from such a contract.[45]

4.3.2 Costs of Policy Option 2 'Entry-exit system'

- '*Financial costs'.* The cost estimates for an entry-exit system with biometrics in the US are around $15 billion, covering the introduction and operation of appropriate technology in all consular posts, as well as entry and exit posts. Should a similar policy option be chosen, it can be anticipated that similar costs would apply to EU entry-exit system.

[45] VIS feasibility study identified that there are 4 suppliers competing for very large systems among which there is one European company.

- '*Opportunity costs'*. Opportunity costs for visa applicants can be expected, as applicants would have to travel to consular posts to provide biometric data.[46] Also time will be lost at entry and exit points by providing and checking biometric data. Additional costs for legitimate travellers would also be incurred due to the travel to consular posts to have the biometric data taken. If it were assumed that one additional person day per visa application would be required, the opportunity cost might be around €50 euros, and the additional average travel cost of €20. This would be in addition to the current average €50 visa application charge. If these assumptions are accepted, the additional costs of VIS for travellers, particularly the indirect costs (time and travel), would be considerable, around €70 additional cost per visa application.

In the current situation, the majority of visa applicants travel to the consular authorities in person to submit a visa application and undergo a personal interview. It is difficult to generalise, but if the following were assumed:

- 40% of visa applicants submit visa applications via post or travel agencies[47];
- Frequent travellers have to provide biometric data only once;
- Frequent travellers are estimated at 20-30%;
- An additional 10-20% of visa applicants would also have to travel to the consular posts to provide biometric data.
- For 20 million visa application requests a year in 27 Member States[48], the additional opportunity costs for this group of visa applicants would amount to €140-280 million.

In addition, trials in the US have shown that, on average, 15 seconds are added to entry procedures when biometric data of travellers is taken. Considering that around 20 million visa requests are estimated as from 2007 (covering EU25 and Iceland and Norway), the taking of biometrics at entry points for visas holders could take travellers' time equivalent to around 14 years in each year of operation of such system.[49] If an assumption is made that on average the opportunity cost of a day lost would be around €50, the opportunity cost for giving biometric data at entry and exit points could be around €250,000.

- *'Retaliation costs'*. Retaliation to entry-exit system with biometrics by third countries currently requiring visas for visitors from the EU should be

[46] An assumption is made that citizens from third countries which do not require a visa to enter the EU (non-visa nationals) will not be subject to biometric checks.

[47] This is the latest statistics from the consulates in Russia and Casablanca.

[48] 20 million visa requests a year are estimated to occur as from 2007 in EU25 and Norway and Iceland. This is based on extrapolation of figure of 12 million visa requests in 2001.

[49] This presupposes that 25% of 20 million visa requests will not be granted, based on current trends. Also, all 15 million visa holders would actually travel to the EU. 15 seconds of delay on entry point for giving biometric data would amount to approximately 2,604 days of person's time, which is about 7 years of person's life, for 15,000,000 travellers. One could assume that similar delays would experienced when giving biometric data in the exit procedures. So the total amount of time spent giving biometric data could be around 14 years.

considered as a risk. At the moment, in response to the introduction of US VISIT, only Brazil introduced retaliatory measures by fingerprinting and photographing Americans arriving at Brazilian airports. Should at least some degree of retaliation occur, it could impose considerable costs on EU citizens (time lost travelling to the consular post, actual time giving biometrics at the consular post, entry and exit point). If similar reciprocal measures are taken, it could also lead to a situation where EU citizens' personal data is taken and stored by authorities in the countries which do not have the adequate data protection mechanisms. The EU would also have to apply considerable leverage to negotiate adequate protection mechanisms for its citizens. This could be problematic, given that it would be the EU that was initiating the system of taking biometric data from foreign visitors requiring visas. However, the risk of such retaliation would be reduced if biometric identifiers are also introduced into all EU passports.[50] In effect, EU and third country nationals would be treated in the same way, in being required to provide biometric data, albeit at different stages in the process.

- '*Reductions in business travel and tourism'*. Due to opportunity costs for visa applicants and perceived invasion into privacy and human rights, some reductions in business travel and tourism can be anticipated. Contributions from visa travellers to overall tourism flows into Europe are relatively small at the moment, but expected to grow substantially in the medium and long term. In percentage terms, passenger volumes into the EU from countries whose citizens require a Schengen visa may not appear to be very substantial.[51] However, the overall numbers are still substantial (around 110 million people). Also, in the longer term, growth of tourism from countries such as China and Russia is anticipated to make a substantial contribution to the tourism revenues in the EU.[52] Should the introduction of an Entry/Exit system of the sort envisaged result in a reduction in travel from third country nationals requiring a visa occur, there would inevitably be some impact on the tourism industry in the EU.

Evidence about emerging impacts of US VISIT on reductions in business and tourism is not clear-cut, not least since it has only been operational since January 2004. On one hand, the overall trend since 11 September 2001 is of declining travel to the US. Visa applications in 2003 were down over 32% since 2001 and international tourist arrivals in 2002 were down by 7% compared to 2001.[53] However, most recent figures suggest that since its introduction, the US VISIT system does not seem to have

[50] This is currently in the proposal stage, see Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports, COM(2004) 116 final, 18 February 2004.

[51] International tourist arrivals in the EU from Americas constituted 13.5% of all arrivals, from Other Europe 13.2%, EFTA countries 4.3% and from Asia, Oceania and Africa 8.9% in 2001. The largest number of arrivals (58.9%) in 2001 was internal, from other EU countries. It could be therefore assumed that around 20% of travellers, or around 110 million people, come from the third countries whose citizens require a visa to enter the territory of Schengen States. Source: European Business, Facts and Figures, Panorama of the European Union 2003, Office of Official Publications of European Communities, Luxembourg, 2003.

[52] World Travel Trends, 2003 – 2004, Forecast Forum: WTM Global Travel Report.

[53] World Tourism Organisation World Tourism Barometer, Volume 2, No. 1. January 2004; The 9/11 Commission Report.

affected tourist numbers.[54] One potential area of negative impacts appears to be a reduction in the numbers of foreign students coming to study into the US.[55]

Based on the available information, it is very difficult to predict whether there would be any reduction in travel to the EU, as a result of this option. Many people travel to the EU because they need to do so for essential business or for employment purposes - these may be expected to continue to travel even subject to additional cost and inconvenience. Others do so as tourists, and might decide to visit places where they do not experience costs and inconvenience of the sort envisaged under a VIS. However, third country nationals travelling to other countries like the US will be familiar with the security and other operational procedures in connection of collecting biometric data, and as more countries begin to incorporate this into their passports, requirements at visa application stage may become more accepted.

An entry-exit system has also to be viewed in the light of general trends in travelling patterns. In the light of emerging new cost-effective technologies, such as video conferencing, physical travel, especially long-haul travel, could be expected to decrease. A decrease in travel could also be expected as a consequence of traveller concerns over the safety and security of flying. A system of better entry-exit controls could assuage such fears by reassuring travellers that, as a consequence of entry-exit system, authorities would have better tools to prevent known terrorists from travelling to the EU.

- '*Impact on privacy and human rights'*.[56] The impact of an entry-exit system with biometrics on privacy and human rights would be extensive, and there would be a substantial need to meet personal data protection requirements. The collection, storage and use of biometric data of all travellers applying for a visa, entering and exiting the territory of Schengen states would raise concerns over the proper use and protection of personal data of travellers. The principles of proportionate and fair use of personal data and high security in the system would have to be implemented in full.

The impact in the negative case scenarios could be quite substantial. Personal data entered and processed in the entry-exit system could be open to unauthorised access and alterations either by authorities not authorised to do so or by criminals who would be eager to steal the identities of legitimate travellers or correct the record of their own personal data. The impact of such identity theft and abuse of the system could be

[54] The number of visitors from Asia increased by 43 per cent over June 2003 and by 32 per cent for the first six months of 2004. Arrivals from South America increased by 16 per cent over June 2003, led by Venezuela and Colombia, which were up 22 per cent and 20 per cent respectively. The number of visitors from South America increased by 12 per cent for the first half of 2004. Source: Office of Travel and Tourism Industries 2004 Monthly Tourism Statistics: http://tinet.ita.doc.gov.

[55] The applications from overseas students seem to have declined by 17.6% in 2004 compared to the previous year figures. See 'US Visa Worries Deter Foreign Students', in The Financial Express, Vol XI, No 252, 31 July 2004.

[56] The term 'privacy and human rights' is used here to refer to the right of a person to the protection of personal data concerning him or her. "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". (Article 8, Charter of the Fundamental Rights). 'Privacy and human rights' also refers to the right to respect for individual's private and family life (Article 7, Charter of the Fundamental Rights).

compared to the increasing identity and credit card fraud in the EU.[57] The positive impact of introducing one system to perform checks on travellers would be an orderly and coherent exchange of information under one set of legal rules, independent supervision and technical security arrangements.

The impact on privacy of visa applicants would also depend on the following operational choices in the implementation of an entry-exit system:

- The kind of biometric data collected in the system. It can be expected that inclusion of biometric data in the form of fingerprints would have a much more substantial impact than inclusion of photographs in the system. Fingerprinting is perceived as a much more intrusive technology, compared to photographs, which has become a standard feature of all official identification documents. Fingerprinting, at least in some countries, has a low social acceptability, being associated with the law enforcement and identification of criminals.

- The length of storage of personal data in the system. The longer personal data is stored in the system, the bigger the impact on privacy would be for the visa applicants.

- The access rights. The greater number of authorities having access to the personal data stored on the system would mean greater impact on privacy of the individuals.

The principles of proportionality and necessity of processing of personal data is also relevant considering the impacts on privacy of individuals. The proportionality of data processing suggest the processing of data commensurate with the objectives of such a system and the scale of problems in the current situation (which are outlined in section 1). In this respect, the inclusion of biometric data poses a fundamental question over the proportionality and necessity of such action, in relation to the problems identified. The inclusion of biometric data would allow authorities to confirm quickly and precisely the identity of visa applicants, which would help to prevent visa application fraud, visa shopping and travel document fraud, improve the efficiency of border checks, help to identify apprehended illegal migrants who have previously applied for a Schengen visa, and prevent known terrorists or other criminals from travelling. Biometric data would also help to facilitate repeat applications from regular travellers, as their identity will confirmed with certainty and visa application history available to consular authorities of all Member States.

However, the inclusion of biometric data also poses a danger that authorities would come to rely completely on the biometric data in the identification and verification process. This could have a negative impact in case of system mistakes, e.g. wrong identification of an individual. Such negative impact would be mitigated if an independent data protection supervisory authority is established, and individuals are granted a right of access to their records and a right to appeal to the independent authority. The data protection considerations are assessed in detail in the Annex 3.

[57] A study in the UK estimated the annual costs of identity fraud to the economy to be in the region of £1.3 billion. It has also pointed out that 'the theft of an individual's identity is a harrowing experience for the victim and for individuals, the experience of identity theft can touch centrally on the victim's relation to the world, … Victims may need time to rebuild their reputations and their credit histories.' See Identity Fraud: a Study, July 2002, Home Office, p. 7.

4.4 Policy Option 3 'VIS without biometrics'

4.4.1 Benefits of Policy Option 3 'VIS without biometrics'

- *'Efficiencies in implementation of common visa policy'*. The introduction of 'VIS without biometrics' would meet the objective of facilitating the implementation of common visa policy through better exchange of information about visa applications. It would ensure that records about visa applications, currently stored by the authorities of Member States where the visa was issued, are available to the consular authorities in all Member States. 'VIS without biometrics' would have beneficial institutional impacts, such as increased exchange of information and co-operation, which will improve the implementation of Common Visa Policy.
- *'Facilitation of implementation of Dublin II regulation'.* The 'VIS without biometrics' option would not improve the current situation where Member States do not have efficient means to check whether an asylum applicant has had a visa issued by another Member State, verify the identity of the person, and find out how long the validity of the visa is/was. All this information is required to identify the Member State responsible for the examination of asylum application. In the 'VIS without biometrics' option, the lack of biometric information would not improve the identification of asylum seekers, who often do not have any travel documents with them.
- *'Reductions in fraud and visa shopping'.* Some reductions in visa application fraud and visa shopping could be expected as comprehensive records of visas issued (as well as visas cancelled, revoked, or annulled) would be kept electronically and shared across the Member States. This would mean that consular authorities in all Member States would have regular and systematic access to the records of past visa applications. When a third country national 'shops' around for another visa after rejection of an application, his past application record would immediately be available to consular authorities without the need to rely on rejection stamp in the passport to provide this information. However, the absence of biometric data of visa applicant would make it difficult to detect visa application fraud and visa shopping where a false identity is used. Also, verification in the database with 70 million records would become very difficult as there would be too many identical names and the 'hit lists' would be too large.
- *'Increased efficiency of border checks'.* Some efficiencies in border checks can be anticipated. If a border guard has access to the system to check whether a traveller was issued a valid visa, this would improve, to some extent, existing border checks based on the visual inspection and the use of document examination equipment to examine the holder of the passport, passport itself and visa. The accuracy and effectiveness of checks against VIS without biometrics would be limited, however, compared with more reliable checks provided by the inclusion of biometric data.
- *'Reductions in illegal migration'.* 'VIS without biometrics' would have a minor impact in reducing illegal migration. This option would make it difficult to identify those undocumented illegal migrants who are apprehended in the territories of Member States and have previously applied for a Schengen visa. Illegal migrants are unlikely to give their true identity to authorities that would be then unable to verify it in VIS without biometrics.

- *'Contributions towards internal security of the Member States including the fight against terrorism'.* 'VIS without biometrics' would have a minor impact in improving internal security and reducing terrorism. However, terrorists and organised criminals (who are known as such to authorities) are unlikely to give their true identity when applying for a Schengen visa or travelling through external borders, and without biometric data would not be identifiable. The impacts in improving internal security will also depend on whether the terrorists or organised criminals suspect that they are known as such to the authorities.
- *'Increased efficiencies for bona-fide travellers'.* There would be advantages for bona fide travellers as past visa history could be established in VIS without biometrics. This would be especially beneficial for regular travellers who apply for a Schengen visa several times. In such cases, the VIS without biometrics would contain full information about a visa applicant from all the previous visa applications, which would automatically be available to authorities in all Member States. This would enable consular authorities to make better decisions about repeat visa applications and thus result in shorter waiting times for regular travellers. Biometric information to identify bona fide travellers would not be needed, as they are unlikely to provide false personal information to consular authorities.
- *'Other spin off benefits including the impacts on the EU IT industry.'* Some small stimulus for IT industries can be anticipated given any information exchange system introduced in 3,500 consular posts and all the border posts would be fairly extensive.

The possibility also needs to be considered that, given the financial and exchange of information advantages of doing so, Member States might decide to pool resources and proceed with common visa application centres, at least in posts where this is operationally feasible.

4.4.2 Costs of Policy Option 3 'VIS without biometrics '

- '*Financial costs'*. 'VIS without biometrics' would carry a medium financial cost.

  – To the Community budget, the cost is estimated to be €30 million in 2004-2006 (one-off investment), and €8 million a year for running the system thereafter.[58] These costs would cover the operation of central part of the VIS without biometrics system.

  – It has proved difficult to obtain the cost estimates for the operation of such a system directly from the Member States. VIS feasibility study estimated that the expenditure for a medium-sized visa issuing office for alphanumeric data and photos would be €4,000 one-off investment costs and €2,000 annual operational costs. Given that there are around 3,500 consular

[58] DG JHA estimates, provided in the financial statement annexed to the proposal for the Council Decision 2004/512/EC.

posts of EU Member States worldwide, such costs would come €14 million one-off investment costs and €7 million annual operational costs.[59]

- '*Opportunity costs'*. No additional opportunity costs for visa applicants are expected, as there would be no change from current visa application processes. The personal information of visa applicants would be collected, processed and stored in the same way as in the present situation.
- *'Retaliation costs'*. No retaliation is anticipated, as there would be no change from current visa application process. The fact that Schengen States would automatically share information about all visa applicants should not evoke any negative reactions from third country countries whose nationals are required to obtain a visa. Introduction of VIS without biometrics would facilitate the exchange of information to implement common EU visa policy which third countries so far have no objections against.
- '*Reductions in business travel and tourism'*. No reductions in business and leisure travel are anticipated, as there would be no change to the current situation in visa application process.
- *'Impact on privacy and human rights'.* Some impact on privacy and human rights of visa applicants could be expected. VIS without biometrics would be a new system of automatic data processing, and all the data protection considerations, such as rights of data subject, would have to be implemented. The introduction of VIS without biometrics would entail some change to the current situation in the visa application process, as information about visa applicants would be shared between all the Member States and amongst a greater number of authorities in the Member States than so far.[60]

4.5 Policy Option 4 'VIS with biometrics'

4.5.1 Benefits of Policy Option 4 'VIS with biometrics'

- *'Efficiencies in implementation of common visa policy'.* The introduction of 'VIS without biometrics' would meet the objective of facilitating the implementation of Common Visa Policy through better exchanges of information about visa applications. It would ensure that records about visa applications, which are currently stored by the authorities of participating Member States where the visa was issued, are available to the consular authorities in all Member States. 'VIS with biometrics' will provide a strong impetus for improvements in the implementation of common visa policy and institutional co-operation through joint consular activities in third countries. The possibility also needs to be considered that given the high costs of VIS with biometrics implementation, Member States might decide to pool resources and proceed with common visa application centres, at least in posts where this is operationally feasible.

[59] This calculation is based on presumption that all consular posts are medium-sized, which does not reflect the situation in all consular posts.

[60] However, in the current Schengen visa application form (point 44) the visa applicants consent to the following use of their personal data, ' any personal data concerning me which appear on this visa application form will be supplied to the relevant authorities in the Schengen states and processed by those authorities, if necessary, for the purposes of a decision on my visa application. Such data may be input into, and stored in, databases accessible to the relevant authorities in the various Schengen states.'

- *'Facilitation of implementation of Dublin II regulation'.* The 'VIS with biometrics' option would bring substantial improvements to the current situation where Member States do not have efficient means to check whether an asylum applicant has had a visa issued by another Member State, verify the identity of the person, and find out how long the validity of the visa is/was. All this information is required to identify the Member State responsible for the examination of asylum application. In 'VIS with biometrics' gathered at visa application stage, the biometric information would provide authorities with means to identify an asylum seeker, who often does not have travel documents, if he has been issued a Schengen visa in the past.
- *'Reductions in fraud and visa shopping'.* Very significant reductions in fraud and visa shopping might be anticipated, as it would be possible to identify a person making applications in several consulates, despite attempts to conceal true identity or use another identity. Without biometrics it would be virtually impossible to identify a person in a database with 70 million records with a common name, in particular taking into account the different ways of spelling those names, and knowing that in some countries the date of birth is an estimated year without a day and a month. With the use of biometric data, it would be possible to identify a person irrespective of the spelling of the name or of other personal data. Biometrics might not identify the 'true' identity of the person, but it would fix an identity to the person who applies for a visa. On the next application, if another identity were used, this would be discovered, using the biometric data, and enabling relevant further enquiries to be made.
- *'Increased efficiency of border checks'.* Very significant increases in efficiency of border checks might be anticipated in the VIS with biometrics. The use of biometric data would ensure that the person who is travelling with the visa is the same person for whom the visa was issued, and thus confirm the identity of the traveller.
- *'Reductions in illegal migration'.* VIS with biometrics would have some impact on illegal migration. Undocumented illegal migrants who are apprehended in the territory of Member States and have previously applied for a visa would be easily identified with the help of biometric data. This would be of value not only in checking whether they entered lawfully, with a visa, but also in documenting them for removal.
- *'Contributions towards internal security of the Member States including the fight against terrorism'.* The improvement of the assessment of visa applications including the consultation between central authorities, and the verification and identification of applicants at consulates and at border checkpoints would contribute considerably to the internal security of the Member States and towards combating terrorism, which constitutes a horizontal objective and basic criterion for the common visa policy. Biometric information would allow identification of visa applicants, even if they use other identities to apply for subsequent visas or cross external EU borders. Concerning the fight against terrorism and organised crime, this impact would occur only if terrorists and organised criminals are known as such and they are nationals of third countries who require a visa to enter the EU. In addition, the effects would be limited and dependent upon the effectiveness of instruments in Policy option 1 'No VIS' because:

- Terrorists may obtain visas and then enter, in a false identity, with "genuine" documents supplied by states prepared to assist them;

- They (and criminals) may enter clandestinely or with a skilled falsification of a passport for which no visa is required; and

- The ability to identify them is dependent upon prior information about them (biometric or otherwise) being available to the relevant authorities.

- *'Increased efficiencies for bona-fide travellers'.* There would be substantial advantages for bona fide travellers requiring visas as past visa history could be established in 'VIS with biometrics'. [61] This would be especially beneficial for regular travellers, who make repeat applications for Schengen visas. The main benefit from the establishment of VIS would be for repeat visitors in terms of simplification of repeat visa applications, which is a welcome development. VIS will have no benefits for the first time traveller. In such cases, the 'VIS with biometrics' would contain full information about a visa applicant from all the previous visa applications, which would automatically available to authorities in all Member States. This would enable consular authorities to make better decisions about repeat visa applications, thereby resulting in shorter waiting times for regular travellers. An additional advantage of 'VIS with biometrics', as against 'VIS without biometrics' is that biometric information would enable the identification of bona fide travellers almost beyond any doubt, thus reducing the possibility of fraud and abuse of the visa system. This would be offset, however, by the inconvenience suffered by bona-fide applicants having to provide biometric data, and submitting to close examination at border checkpoints.

- *'Other spin off benefits including the impacts on the EU IT industry.'* A strong stimulus for the IT industry may be anticipated, given the costs associated with this policy option. VIS would require the installation and running of state-of-art equipment to capture biometrics and perform checks of travellers in all consular authorities of Member States. Such installation and training would occur in 3,500 consular posts, with 12,000 users, as well as all the EU external border posts. However, as US companies dominate the biometrics industry, it is not necessarily EU IT industry that would benefit from such a contract.[62]

4.5.2 Costs of Policy Option 4 'VIS with biometrics '

- '*Financial costs'*. 'VIS with biometrics' would carry significant financial costs.

[61] Indeed, this is already being tested by pilot projects in several EU countries. Germany has tested a border control system based on iris recognition technology at the Frankfurt airport. Also, in June 2004, the UK announced the award of a contract for a project, named IRIS (Iris Recognition Immigration System), which will store and verify the iris patterns of specially selected groups of travellers (foreign nationals who live permanently in the UK, are regular travellers or work permit holders and have a track record of complying with the country's immigration laws). Passengers enrolled on the system will be able to enter the UK through a special immigration control to speed up immigration control procedures.

[62] VIS feasibility study identified that there are 4 suppliers competing for the design and implementation of very large IT systems, among which there is one European company.

	One-off investment costs	Annual operational costs
Costs for the Community	€93 million	€14-16 million
Costs for the Member States (national systems)	€186 million	€49 million
Total costs (for VIS and consulates)	€246-256 million	€55-57 million

- It is estimated that for the Community budget the 'VIS with biometrics' would cost €93 million in 2007-2011 for investment costs, and afterwards €14-16 million a year for operational costs.[63] The estimates for the Community budget cover the costs for the development of the central part of the VIS, and do not include estimates for the national systems.

- Two Member States provided estimates of costs of installing and running VIS with biometrics in their consular posts. France (one of largest visa issuing Member States) indicated that the one-off investment costs would be around €11 million, with the subsequent annual operational costs of €1 million. Sweden (a Member State which issues a small number of visas) estimated that the one-off investment costs would be around €2.8 million with annual operational costs of €2.5 million. The average of these two available estimates would be around €6.9 million one-off investment costs and €1.8 annual operational costs. For 27 participating Member States, such costs would amount to €186 million one-off investment cost and €49 million annual operational costs. Such estimates are however to be treated with caution, given the lack of more comprehensive financial assessments from a greater number of Member States.

- Another indicator of financial cost may be gleaned from the VIS feasibility study.[64] It estimated that the expenditure for a VIS with biometrics (including alphanumeric data, photo, biometrics, scanned supporting documents) in a medium sized visa issuing office would be €14,000 investment costs and €5,000 annual operational costs. Given that there are currently estimated to be 3,500 consular posts of EU Member States worldwide, the investment (one-off) costs would be €49 million and annual operational costs would be €17.5 million.

- These estimates also cover investment and operational costs only in the consular posts, and do not include costs of VIS with biometrics for national central authorities and for border crossing points and other authorities. For these cost estimates are not available.

- '*Opportunity costs'*. Extensive opportunity costs to visa applicants are anticipated (similar to the costs in the entry-exist system with biometrics option). The additional costs for legitimate travellers would also be incurred due to the travel to consular posts to have the biometric data taken. If it were

[63] These are the latest estimates provided by DG JHA. They include the costs for operating VIS without biometrics and the additional costs for VIS with biometrics.

[64] VIS feasibility study final report, DG Justice and Home Affairs, April 2003.

assumed that one additional person day per visa application would be required, the opportunity cost might be around €50 euros, and the additional average travel cost of €20. This add-on cost of €70 would be in addition to the current average €50 visa application charge.

In the current situation, the majority of visa applicants travel to the consular authorities in person to submit a visa application and undergo a personal interview. It is difficult to generalise, but if the following were assumed:

- 40% of visa applicants submit visa applications via post or travel agencies[65];
- Frequent travellers have to provide biometric data only once;
- Frequent travellers are estimated at 20-30%;
- An additional 10-20% of visa applicants would also have to travel to the consular posts to provide biometric data.
- For 20 million visa application requests a year in 27 Member States[66], the additional opportunity costs for this group of visa applicants would amount to €140-280 million.

- *'Retaliation costs'*. Retaliation to 'VIS with biometrics' by third countries currently requiring visas for visitors from the EU should be considered as a potential risk. As noted in section 4.3.2 above, to date only Brazil has introduced retaliatory measures against the US VISIT system, by fingerprinting and photographing Americans arriving at Brazilian airports. Should at least some degree of retaliation occur, it would impose considerable costs and inconvenience on EU citizens (time lost travelling to the consular post, actual time giving biometrics at the consular post).[67] If similar reciprocal measures were taken, it could also lead to a situation where EU citizens' personal data is taken and stored by authorities in the countries which do not have the adequate data protection mechanisms. The EU would also have to apply considerable leverage to negotiate adequate protection mechanisms for its citizens. However, such a retaliation risk would be reduced if biometric identifiers were also introduced into the EU citizens' passports, as it would entail no differentiated treatment between EU and third country citizens.[68] It should also be borne in mind that instead of taking the biometric data of EU citizens (which might be too expensive a measure for less developed countries), third countries could also just impose an increased

[65] This is the latest statistics from the consulates in Russia and Casablanca.

[66] 20 million visa requests a year are estimated to occur as from 2007 in EU25 and Norway and Iceland. This is based on extrapolation of figure of 12 million visa requests in 2001.

[67] As an example, it is possible to consider a scenario where a country popular with tourists from the EU (2 million visitors a year) introduces a system of biometric identification of visa applicants. EU citizens would have to travel to the embassy to give biometrics (currently applications are mostly submitted by post or via travel agent). The average opportunity cost for such a travel would be one day (€200 average), and the travel costs could be estimated at average €50. This would entail an additional cost for EU citizen in the region of €250 for getting a visa. With 2 million visitors, the additional costs of opportunity time and travel expenses would amount to € 500 million annually.

[68] This is currently in the proposal stage, see Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports, COM(2004) 116 final, 18 February 2004.

levy for processing visa application, which would result in additional direct costs to an EU citizen.

- '*Reductions in business travel and tourism'*. Due to opportunity costs for visa applicants and perceived invasion into privacy and human rights, some reductions in business travel and tourism might be anticipated. The (albeit limited) evidence of reactions to US VISIT system has been considered in the section 4.3.2 above. This does appear to suggest that in the short term some reductions in travel may be expected, as a result of the introduction of fingerprinting travellers. However, it is considered that in the long term such a negative impact might be expected to diminish, as travellers became accustomed to the requirements of VIS with biometrics, and indeed to use of biometrics in their own documents.

It can be expected that most genuine visitors will have nothing to hide and will provide biometric data. They would accept a trade-off between providing personal information and safer and easier travel into Europe. If VIS provides efficiency in the process, visa travellers would welcome this. Small number of people will find the taking of biometric data intrusive and unacceptable and may refrain from travelling into Europe. Therefore, authorities should research particular markets, and cultural and religious sensitivities to biometric data.

- 'Impact on privacy and human rights'. Impact on privacy and human rights would be extensive, and there would be a substantial need to meet personal data protection requirements. The collection, storage and use of highly personalised and sensitive data, such as biometrics of all travellers applying for a visa to enter the territory of Schengen States, would raise concerns over the proper use and protection of personal data of travellers on such a massive scale.[69] The principles of proportionate and fair use of personal data and high security in the system would have to be considered carefully. In particular, the principles of proportionality and necessity of the storage and processing will have to be implemented in full. It is also worth noting that these parameters depend on what biometrics are taken, for how long they are stored and what authorities will have access to the data (these questions are explored in greater detail in sections 5.5-5.8 and Annex 3 to this report).

The impact in the negative case scenarios could be quite substantial. If there would be no appropriate safeguards on data security in place, personal data entered and processed in VIS with biometrics could be open to unauthorised access and alterations either by authorities not authorised to do so, or by criminals who would be eager to steal the identities of legitimate travellers or correct the record of their own personal data. The impact of such identity theft and abuse of the system could be compared to the increasing identity and credit card fraud in the EU.[70] There could also be cases

[69] Indeed, privacy and data protection concerns surfaced as a major criticism of VIS with biometrics in the public consultation process during the course of this EIA. In the words of one NGO, VIS (and SIS II and PNR as well) 'would introduce the surveillance of the movements of everyone in the EU - citizens, legally resident third-country nationals, visa entrants and irregular migrants - and the storage of their personal data on an unprecedented scale.' See Statewatch analysis, From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained, February 2004. However, in VIS only the data of visa applicants and of EU persons issuing invitations or liable to pay the costs of the stay would be stored.

[70] A study in the UK estimated the annual costs of identity fraud to the economy to be in the region of £1.3 billion. It has also pointed out that 'the theft of an individual's identity is a harrowing experience for the victim

where mistakes are made on the basis of VIS data, such as false matches of a traveller to a person with criminal record. In such cases, the consequences for a traveller could potentially be extremely grave, resulting in a rejection of a visa application or refusal of entry into the territory of Schengen States.

Such extreme negative impacts would be mitigated if the person concerned were to be provided with precise information on the grounds for taking such a decision, and were allowed to clarify the circumstances without delay. In practice, this would also entail a right of access to their personal data and a right to object with data controller and to appeal to an independent supervisory authority. On the positive side, the beneficial impact of introducing one system to perform checks on visa applicants (in place of various arrangements currently in place) would be an orderly and coherent exchange of information under one set of legal rules, independent supervision and technical security arrangements.

4.6 Summary

The benefits of the four policy options are summarised in Table 4.1 and the costs are summarised in table 4.2.

and for individuals, the experience of identity theft can touch centrally on the victim's relation to the world, … Victims may need time to rebuild their reputations and their credit histories.' See Identity Fraud: a Study, July 2002, Home Office, p. 7.

Table 4.1 Summary of costs associated with policy options

	Financial costs	Opportunity costs for visa applicants	Retaliation costs for EU travellers	Reductions in business travel and tourism	Impact on privacy and human rights
'No VIS'	-	-	-	-	-
'Entry-exit system' (with biometrics)	√√√√	√√√	√	√	√√√
'VIS without biometrics'	√	-	-	-	√
'VIS with biometrics'	√√√	√√	√	√	√√√

√√√√ Exorbitant

√√√ Very significant

√√ Medium

√ Small

- No change from present situation

Table 4.2 Summary of benefits associated with each policy options

	Efficiencies in implementation of Common Visa Policy	Facilitation of Dublin II regulation	Reductions in fraud and visa shopping	Increased efficiency of border checks	Reductions in illegal migration	Contri-butions towards internal security	Increased efficiencies for bona fide travellers	Other spin offs
'No VIS'	-	-	√*	√*	√*	√*	-	-
'Entry-exit system'	√√√	√√√	√√√	√√√	√√√	√√	√√√	√√√
'VIS without biometrics'	√√	-	√√	√√	√	√	√√	√
'VIS with biometrics'	√√√	√√√	√√√	√√√	√√	√√	√√√	√√√

√√√ Very significant

√√ Medium

√ Small

√* Impact conditional on the effectiveness of current developments and developments planned (including SIS II)

-No change from present situation

By way of summary, Table 4.3 presents the main advantages and drawbacks of the four policy options.

Table 4.3 Summary of advantages and drawbacks of policy options

Policy options	Advantages	Drawbacks
'No VIS'	• Low financial cost	• No improvements
'Entry-exit system' (with biometrics)	• Substantial improvements in addressing problems in current situation	• Exorbitant financial costs • Extensive impacts on data protection and fundamental rights. • Risk of retaliation
'VIS without biometrics'	• Moderate financial cost • Non-financial costs low (opportunity costs for visa applicants) • Some improvements in the current situation	• No reliable person identification and verification • No contribution to fight against illegal migration
'VIS with biometrics'	• Substantial improvements in most domains	• High financial costs and high indirect costs • No data on exits • Extensive impacts on data protection and fundamental rights. • Risk of retaliation

4.7 Proportionality and added value of European policy

Table 4.4 summaries the assessment of the options in terms of their proportionality and European added value. Proportionality concerns whether the costs of the option is proportional to the scale and nature of the problems addressed and the likely benefits that will result. The European added value assessments consider whether action at the EU level is appropriate.

Table 4.4 The proportionality and added value of the policy options

	Proportionality	European added value
'No VIS'	Does not address all of the political objectives set and only some improvements in the problems in the current situation could be anticipated	None
'Entry-exit system' (with biometrics)	Substantial improvement, however, a huge organisation step change from current situation, risky and extremely costly to implement	As VIS with biometrics but also enables comprehensive immigration controls
'VIS without biometrics'	Moderate financial costs but addresses the problems in the current situation and political objectives set to a certain degree	Facilitates exchange of information on visas on a regular and comprehensive basis to enable implementation of common visa policy
'VIS with biometrics'	High costs but would tackle many of the problems identified and meet political objectives set	Facilitates exchange of information on visas on a regular and comprehensive basis to enable implementation of common visa policy Identification of visa applicants with the use of biometrics enables reliable and immediate exchange of information Contributes to an effective return policy

5 DETAILED ASSESSMENT OF POLICY OPTION 3 (VIS WITHOUT BIOMETRICS) AND POLICY OPTION 4 (VIS WITH BIOMETRICS)

5.1 Introduction

On the basis of the assessment in Section 4, there is a strong case for eliminating the first two policy options from further consideration.

If a visa information system were not introduced, there would be no improvements in the exchange of visa application information between consular authorities of Member States. The absence of a visa information exchange system would not address some of the most pressing issues, such as visa shopping and visa fraud. Furthermore, the development of Common EU Visa Application Centres, which would address the visa shopping problem and facilitate exchanges of information, is unlikely in the short and medium term.

An EU entry-exit system, incorporating biometrics for visa applicants, would provide a continuum of measures to control the movements of third country nationals, from a visa application stage through arrival at external border to leaving the territory of Schengen state. Such a system would enable much more efficient and effective border controls to be operated. There would be improvements to immigration control arrangements, overall, due to the existence of more comprehensive records. In some measure, such records would contribute to better checks on terrorists, potential terrorists and major criminals. However, without arrangements to gather and store visa data on a Schengen-wide basis, it would not achieve all of the main objectives of the Council Conclusions on the development of the VIS on 19 February (6535/04), for example, by contributing to the improvement of consular information and the exchange of information between consular authorities, helping to apply the Dublin II Regulation. It therefore appears to be less advantageous than VIS with biometrics.

In addition, the purposes of entry-exit go far beyond the aims of a visa information system and appear to be disproportionate and excessive. The entry-exit system would also have other implications, such as very heavy costs and would require major financial and institutional investment. It could also potentially could attract same adverse reactions from other States and their nationals as a US VISIT system.

The two remaining policy options are considered to generate benefits commensurate with their costs. However, the relative merits of VIS without biometrics (Option 3) and VIS with biometrics (Option 4) need to be considered in detail.

In addition to the cost-benefit analysis of the two policy options, there are also a number of parameters which will impact on the effectiveness of the two policy options as measured against the political objectives for a visa information exchange system. These parameters are:

- Categories of personal data to be included as well as the question whether the personal data of EU citizens and companies issuing visa invitations should be included;
- Inclusion of biometric data;
- Inclusion of scanned documents;
- Length of retention period of data on the system;
- Issues about access to personal data contained in the system.

5.2 Assessment of costs

5.2.1 Financial costs

	'VIS without biometrics'		'VIS with biometrics'	
	One-off investment costs	**Annual operational costs**	**One-off investment costs**	**Annual operational costs**
Costs for the Community	€30 million	€8 million	€93 million	€14-16 million
Costs for the Member States (national systems)	No estimates	No estimates	€186 million	€49 million
Total costs			€246-256 million	€55-57 million

5.2.2 Impact on fundamental rights of persons

If the principles of data protection legislation are applied correctly[71] in the implementation of VIS, fundamental rights of persons concerning processing of their personal data should be secure. In other words, regardless of whether biometric data is included or not, a visa information exchange system would have to comply fully with the data protection requirements. In particular, the principles of proportionality and necessity of the storage and processing will have to be implemented in full. It is also worth noting that these parameters depend on what biometrics are taken, for how long they are stored and what authorities will have access to the data (these questions are explored in greater detail in sections 5.5 - 5.8 and Annex 3 to this report).

On the positive side, VIS (with or without biometric data) would make it easier to exchange personal information in an orderly manner in a system with legal rules, independent supervision and high technical protection of processing of personal data. However, inclusion of biometric data in a visa information exchange system would be perceived as a major intrusion into the privacy of third country nationals due solely to the fact they want to travel to the EU.[72] This is because:

- The use of biometric data in government databases has a low social acceptability in some countries. Fingerprinting technologies have so far been used primarily in the law enforcement context and the identification of criminals. This is, however, likely to change with the introduction of biometric data in national passports and ID cards, and such plans are under discussion or on the way in Belgium, Denmark, Netherlands, Ireland, Italy, Slovenia and

[71] These are elaborated in Annex 3.

[72] See for example the Opinion 7/2004 of the Article 29 Data Protection Working Party. Such views have also been expressed frequently in the public consultation launched for this EIA.

the UK. The use of fingerprints has a low social acceptability in industrialised countries, in particular, whereas in other countries it is much more widely accepted, as biometric data is often the only means of proving personal identity in commercial (e.g. signing a contract) and public settings (e.g. identification of voters for elections to prevent fraud).

- The collection of biometric data of every third country national who applies for a visa would be one of the first such large-scale databases of biometric data in the EU. This would be mitigated if biometric data started to be used more widely, especially in EU citizens' passports and ID cards.
- There is a risk that consular and other authorities would rely disproportionately on biometric identification techniques in the VIS, to ascertain and verify the identity of visa applicants and travellers. The problems of reliability in the operation of such a large-scale database could potentially create harmful consequences for persons involved, especially in cases of system mistakes. This has also been raised by the Article 29 Data Protection Working Party in its Opinion 7/2004. Such effects would be mitigated by granting third country nationals a right to access their personal data, and a right to object and appeal against misuse of their personal data in the VIS.
- Application of biometric technology in the VIS could have larger negative effects on the persons concerned, compared with the processing of alphanumeric data in VIS without biometrics, if the biometric data is lost, attributed wrongly or otherwise misappropriated. A number of such potential cases could be envisaged, such as when an individual whose fingerprints are collected does not otherwise communicate his real identity, and the "hijacked" identity would then be permanently associated with the fingerprints in question. Alternatively, a system might identify a data subject as someone who is a threat to public security and should not be allowed to enter the territory of a Schengen State. Inclusion of biometric data on the VIS would have negative consequences for bona fide travellers in cases of failed match, mistaken match and stolen biometrics. The possibility cannot be discounted that there would be cases where VIS with biometrics would not confirm the identity of traveller, or confirm an identity incorrectly, or cases where traveller's identity is stolen. Situations can also arise where a person provides biometric data to consular authorities, but fails to provide his true identity. In this case, that set of biometric data would be permanently fixed to an incorrect identity, which might belong to another person.[73] It is difficult to ascertain the number of such cases in the future.
- Given the trust placed in biometric technology, it might be extremely difficult for the bona fide individual to prove his story and clear his name.74 The use of biometric data might create an illusion that the identification and verification of the person is always correct. The data subject may find it

[73] Such concern is also raised by the Article 29 Data Protection Working Party in its opinion 7/2004, adopted on 11 August 2004.

[74] An analogy with credit card fraud and identity theft could be evoked. In such cases, it is extremely prolonged and costly process for the individual whose identity has been stolen to reinstate his good credit ratings and clear his name.

difficult or even impossible to prove the contrary.75 If a second biometric identifier and/or other data were included, these additional search criteria would significantly reduce the frequency of mistakes in the system.

Current evidence about the reliability of biometric data systems and the proportion of failed and mistaken matches in such databases suggests that such cases do occur. The Eurodac database was set up with the accuracy requirement of more than 99.9% certainty for all returned submissions, and with a probability of less than 0.5% of missing match. In other words, the error margin is programmed between 0.1% and 0.5% of transactions in such a database.[76] The possibility of finding the data relating to a specific person in a biometric database would decrease in proportion to the increase in the volume of data that the database contained, even though the search is made by automatic means.[77]

In the VIS with 12 million applications annually, 0.1% error margin could translate into 12,000 cases with false or mistaken identification of visa applicants.

The consequences of such cases for bona fide travellers would be severe as they could result in a rejection of visa application and refusal of entry into the territory of Schengen states. Such negative impacts would be mitigated through informing the traveller immediately about the reasons for such a decision and providing a speedy recourse to access his personal data held on the VIS and clarify the circumstances of individual cases.[78]

5.3 Assessment of benefits

5.3.1 Efficiencies in implementation of EU policies

In both Option 3 and 4, the present fragmentary arrangements for the exchange of information, between Member States would be replaced by a system, which would provide access to the records of visas granted and refused. The arrangements for exchanges of information should also ensure that trends are easier to identify, and that details of forms of deception identified can be passed quickly and efficiently to all participating States. This would lead to more efficient and effective visa processing. There should also be better management information dissemination to Member States, enabling them to produce statistical material quickly and easily.

A VIS, with or without biometrics, would enable collection, assessment, and dissemination of information about trends identified. These might include:

- Different forms of deception used at the visa application stage, for example, the use of falsified letters of invitation for social or business visits, and spurious plans to attend educational courses (sometimes with the

[75] See also Article 29 Data Protection Working Party Working Document of Biometrics, 1 August 2003.

[76] The error margin between 0.1 and 0.5% appears to be routine within the biometric data systems. For industry estimates overview, see 'Biometric cards will not stop identity fraud', in New Scientist, 21 November 2003, and 'Body Check: Biometrics Defeated' by Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, 3 June 2002, in www.extremetech.com.

[77] Opinion 7/2004 of Article 29 Data Protection Working Party, p. 5.

[78] This is a course of action also suggested by the Article 29 Data Protection Party (Opinion 7/2004, p. 7.).

participation of fraudulent educational institutions – which would be identified);

- Routes (including transit points) identified as used commonly by bogus applicants;
- Organisations and individuals found to have facilitated or sponsored intending illegal migrants;
- Details of falsified documents identified – forms of deception used, including types of falsification and documents particularly favoured, and particularly skilful modes of falsification identified;
- Statistics regarding categories of application, and breakdown by nationality of grants/refusals;
- Nationality (and other) profiles of people who have made unsuccessful applications;
- Details of "repeat" applications made – particular nationalities apparently attempting "visa shopping".

In 'VIS without biometrics', the processing of visa applications would be improved through:

- More immediate access to previous applications, whether granted or refused, in any participating State;
- Providing a clear audit trail by demonstrating from beginning to end who dealt with the visa application, what authorities were exercised, at what level.

The establishment and use of VIS for visa issuing has the potential to facilitate the application of common rules, principles and practices in the visa issuing process and border checks at the Member States. The VIS would support the implementation of the common visa policy. Clear unambiguous instructions, with training, for the authorities using the VIS data could lead to the equal and consistent application of the visa issuing rules and border checks of the Member States. There is currently a real risk that visa applicants in analogous situations are treated differently by the authorities in Member States. The number and nature of the supporting documents required for visa application may differ considerably depending on where the application is lodged.[79]

Both policy options have the potential to encourage the consistent application of common rules, principles and practices in the visa issuing process by Member States. However, inclusion of biometrics might provide a stronger stimulus towards joint consular activities, since individual Member States might be more willing to pool human and technical resources given the high costs of biometrics in separate consular posts. 'VIS with biometrics' will enable the consular authorities to rely fully on the visa decisions made by other Member States' consular authorities. It could lead to the harmonised justification for issuing (or not issuing) a visa by all Member States.

'VIS with biometrics' would enable precise checks whether a Member State has issued a visa to an asylum seeker in order to determine which Member State will be

[79] Cholewinski, R. (2002) 'Borders and discrimination in the European Union', Immigration Law Practitioners' Association, London, Migration Policy Group, Brussels.

responsible for examining the asylum application, and thus help to implement Dublin II Regulation.[80] In cases where an asylum seeker entered Schengen with a visa issued by a Member State, but applied for asylum without any travel documents, the use of biometric data would help to determine the identity of the asylum seeker, and which Member State had issued a visa to him.[81] A positive "hit" in the VIS in such cases would provide access to all the personal data needed to identify such a visa applicant (such as name, personal details, nationality), the consulate that issued a visa in the first instance as well as other information which might help to investigate the asylum claims (such as any supporting documents if such functionality is included in the VIS).

Checks to see whether an asylum applicant had sought a visa at any stage would clearly be facilitated by 'VIS with biometrics'. This might demonstrate that claims made in the asylum application are false – it might equally lend weight to the claims of persecution made. In particular, details of a valid passport held at any stage would prove invaluable, either in enabling the applicant to be properly documented if asylum is granted, or in documenting him for removal. If the person has not advanced true details of his identity and nationality or citizenship, when seeking asylum, biometric data held would enable him to be identified. However, 'VIS with biometrics' would only assist in such cases if the applicant has sought a visa at some stage.

5.3.2 Reductions in fraud and visa shopping

In 'VIS without biometrics' it would be possible to discover whether a person had previously applied for a visa only if the person gives his true identity and personal data. Inclusion of biometric data would allow authorities to confirm identities of visa applicants with speed, certainty and precision. In cases where third country nationals have not complied with visa and immigration requirements in the past (and this has been recorded on the VIS), this information will be instantly available to the consular authorities. This would reduce the opportunities for subsequent visa application fraud and prevent third country nationals from visa shopping.

5.3.3 Increased efficiency of border checks

In 'VIS without biometrics', there would be continued difficulties in detecting counterfeit and forged visas, those issued to one person, and transferred to the travel document of another, and travel documents (containing a visa) produced at the border control by an imposter. Only the ability to check biometric data would ensure a more reliable verification that the person who is travelling with the visa is the same person who was issued a visa.

The inclusion of biometric data in the VIS would have an impact on the business process of border checks and crossings. If, under VIS, checks of biometric data are not made on a routine basis (but selectively) on the basis of judgement of a border guard, the possession of a valid visa would facilitate passage of third country nationals through the border controls. Where cases are "selected" for further examination, further enquiries will be facilitated by having a VIS, particularly one with terminals at

[80] According to the hierarchy of criteria in the Dublin II regulation, Member State which issued a visa to a third country national is responsible for examining his application for asylum.

[81] Member State which issued a visa might not be the one where the asylum seeker lodges asylum application. In such case, the Member State where he lodges asylum application will then request the Member State which issued a visa to take charge of his application.

the border. Information provided by the individual, for example, regarding declarations made to the visa officer, can be checked quickly and easily. In particular, in cases in which there is reason to believe that the travel document has been altered without authority, it will be possible to check the state of the document, including visas and other endorsements in it, when it left the visa officer.

Similarly, *after-entry checks*, both those in relation to residence permits and other permissions to stay, and in enforcement cases, would be facilitated by the ability quickly and effectively to check details of visas granted or refused to those under enquiry. Details of visa applications made in countries other than that in which the current enquiry is being pursued would be particularly useful.

If VIS with biometrics were in place, and records had been built up, there should be increased confidence for the border guard that the visa in any passport he is examining has been issued in accordance with established criteria, and after access to any previous applications. This should, therefore, reduce the reason for him to question those holding visas. In itself, this would expedite passage through the controls of bona-fide travellers.

The availability of such information might make the border guard more likely to make enquiries when there is no real need to do so, thus resulting in delays. However, this potential problem can be minimised by clear instructions to staff about the circumstances in which further enquiries of this type should be conducted, making it explicit that they should be necessary only on a selective basis.

The introduction of the VIS should therefore make border controls quicker rather than slower. It follows that border checks would be assisted, and improved by the VIS. There should be no adverse effects of having access to VIS records at the border, unless an unduly rigorous approach to checks is made by border control staff, in which case delays could be caused.

5.3.4 Reductions in illegal migration

Neither Policy Option 3 and Policy Option 4 would prevent people from entering clandestinely, nor they would have any effect on people who enter the EU without visas. However, Policy Option 4 (and to a lesser extent Policy Option 3) would assist in dealing with other forms of illegal entry and stay, including overstaying. Illegal migrants would still have to be traced, and where appropriate detained, but the efforts expended on this should be reduced, and the periods of detention involved should be shorter. In addition, inclusion of biometric data would greatly facilitate the identification and documentation of undocumented illegal migrants.

Once illegal migrants are apprehended, biometric data would enable control authorities to check whether the person was previously issued with a visa by a Member State, and help to identify him. In this way, biometric data would speed up the administrative process for identifying and preparing for the removal of illegal migrants. The production to an illegal migrant's own consular authorities, of details of a travel document, valid at the time of issue of the visa, should enable them to respond quickly and positively to a request for a travel document. This is particularly so if the application is accompanied by a scanned photograph of the document(s) originally held by the applicant, and/or biometric data. In this context, it may be noted that following a successful pilot project in Sri Lanka, the United Kingdom announced in January 2004 plans to require people

from Djibouti, Eritrea, Ethiopia, Tanzania and Uganda, to provide a record of their fingerprints when applying for visas.

VIS with biometrics would also make it more difficult for people to enter a country illegally, for example, by application under different identities or by concealment of previous applications, because biometric data would permit identification of such applications quickly and efficiently.

VIS with biometrics may also act as a deterrent to those prepared to conceal a previous application, or a previous occasion on which they have entered or remained illegally. It will quickly become known that an automated pool of biometric and other data will be available to consular staff. In addition, those involved in organised criminal activity would know that people who may currently successfully conceal previous applications, or indeed previous acts of illegal migration, and whom they assist in their applications, are much more likely to be detected when the VIS with biometrics is in place. However, an increase of clandestine entries into the Schengen territory might be expected.

On the one hand, if the effect of 'VIS with biometrics' would lead to reduced illegal migration in the long term, this would benefit the transport sector, and especially the airlines (which currently under carrier liability legislation have to carry back the illegal migrant when he is turned back at the external EU borders). In the short term, the effect of 'VIS with biometrics' could be that, due to the biometric technologies, more illegal migrants are identified at the external borders, which would entail a cost to the airlines. If the airlines negotiated that the airline staff could not have reasonably identified such cases, this cost to the airlines could be reduced. Otherwise, airlines would have to replicate the biometric check, and install new equipment in the airports.

5.3.5 Contributions towards internal security of the Member States including fight against terrorism

Improvement of the assessment of visa applications, including consultation between the central authorities, and the verification and identification of applicants at consulates and at border checkpoints, contribute to the internal security of Member States, and towards combating terrorism, which constitutes a horizontal objective and basic criterion for the common visa policy. The introduction of a VIS would facilitate the implementation of common visa policy, and thus contribute to the prevention of threats to internal security. Ways in which the common visa policy (and relevant checks) should contribute significantly to internal security and the fight against terrorism include:

- More efficient and effective assessment of visa applications at the consular posts to establish that visa applicants do not threaten internal security, and thus prevent any subsequent risks and threats. In particular, VISION consultation allows checks to be whether other Member States have information to suggest that the visa applicant constitutes such a threat to internal security;
- Verification and identification of travellers with visas at the external border checkpoints, to ensure that only individuals for whom the visa was issued enter the territory of Schengen States.

As indicated above, in Policy Option 3, it will be difficult to identify visa applications by terrorists and organised criminals unless they use their true identity, or an identity known to authorities. However, inclusion of biometric data would enable authorities to confirm the identity of terrorists and organised criminals, when they apply for a Schengen visa, if they are known to authorities already, and if they had made a previous visa application and their biometric data was taken. This might dissuade terrorists and organised criminals from making a visa application.

Terrorists, potential terrorists and major criminals might still succeed in many cases in crossing borders unchallenged, whether concealed in a vehicle or container, or over the "green border." They may also enter with skilfully falsified documents, which purport to show that they do not require a visa, and in the case of terrorists, might succeed in entering with a passport issued in a false identity by officials prepared to assist them.

The circumstances in which VIS would be the most effective in contributing to the improvement of internal security and reduction of terrorism are:

- If terrorists and organised criminals come from countries whose citizens are required to have a visa to enter the Schengen territory; and
- If they are already known to the authorities as risks to internal security (including as terrorists), prior to a visa application.

5.3.6 Efficiencies for bona fide travellers

A reliable link between the holder, passport and visa would be established under the VIS with biometrics. In contrast to the storage of biometric data on the visa chip only, the use of biometric data in the VIS would also establish, with certainty, the visa history of those applying frequently for visas. In cases where third country nationals have complied with immigration and visa requirements in the past, this valuable information would be available to the consular authorities and border check posts. This would enable better informed decisions on issuing visas to frequent travellers, thus cutting down the times of processing visa applications, achieving greater administrative efficiency and facilitating the applicants.

The main benefit for repeat visitors from the establishment of VIS would be the simplification of repeat visa applications. From this point of view, collection and sharing of visa data should be welcomed as facilitation of visa application, as long as data protection is fully enforced.

Any form of VIS should bring more transparency to the visa application process and make it more accessible and easier for visa travellers. Europe must be perceived as a place of welcome, and VIS should not be about policing the issuance of visas, but facilitating the application process and providing ease of access for business and leisure travellers. If consular authorities have access to the right information about the person, especially in the repeat application, that could make the service more professional, more successful and speedier.

It can be expected that most genuine visitors will have nothing to hide and will provide biometric data. They would accept a trade-off between providing personal information and safer and easier travel into Europe. This would be especially so if providing biometric data will mean that subsequent issuing of visa is a ‘stamp of approval’ and

will guarantee entry into the EU. Small number of people will find the taking of biometric data intrusive and unacceptable and may refrain from travelling into Europe. Therefore, authorities should research particular markets, and cultural-religious sensitivities to biometric data.

However, the impact of VIS could be severe for those whose visa applications were previously refused and whose details are entered into the VIS. Visas are refused on a variety of grounds, and individual's circumstances change. If such persons should apply for a Schengen visa at a later stage, their applications might be viewed as doubtful by consular authorities, although the original grounds for a visa refusal (such as an absence of sufficient financial support or suspicions that the person intended to remain as an illegal migrant) might no longer be valid. There could be a risk that the subsequent visa applications would be decided, not on the merits of the application now made to the consular authorities, but on the past visa refusal.

Such an impact would be mitigated through detailed instructions and training for consular staff, and monitoring of visa application decisions, so that all applications are judged on their current merits. This should ensure fairness of the system. Also, providing a third country national with the right to object or appeal against the decision (in accordance with the framework of national law of the Member State to which the application is made) would mitigate such negative effects. Such a negative impact could occur in the implementation of VIS, regardless of whether biometric data is included or not.

In cases of lost or stolen documents after the entry into the Schengen territory, VIS with biometrics would facilitate the identification of bona fide traveller as there would be an automated record, giving full details of the previous application(s).

Although visas may facilitate passage through border controls, and may constitute an assurance (if not a guarantee) that entry will be granted, the need to obtain a visa is normally viewed by the bona-fide traveller as annoying and expensive bureaucracy. Bona fide travellers may well accept that there is a need to strengthen the fight against illegal migration, major crime and terrorism, but many will question whether they should have further, burdensome procedures, such as the need to provide biometric data imposed upon them, particularly since the costs of the additional procedures will almost inevitably increase the cost of visa applications.

Therefore, it is suggested that a committed publicity campaign will be needed, stressing the extent to which a VIS with biometrics will serve the public interest, if bon-fide travellers are to be assured that it is in *their* interests that a new and costly system of this type should be introduced. The policy of transparency and ease for genuine visitors should be explicitly promoted to visa applicants. The publicity campaign should be sensitive and take into account the cultural and social circumstances in different countries. It can be anticipated that in the short term VIS would cause negative impact, and authorities need to be prepared for that through a PR campaign. It should be focused on end-customer, and explain why, for whom, and what benefits the system will bring to the traveller. The example of Brazilian retaliation to US-VISIT shows how disruptive retaliation can be.

5.3.7 Spin off effects and effects on other EU policy areas

VIS with biometrics requires the traveller to come to the consular authority (or other nominated point) in person for the application of visa and submit biometric data. This might mean elimination of the travel agencies from the procedure and subsequent loss of income for them. It has to be stressed, however, that these travel agencies are based outside the EU, so we do not anticipate a direct impact on Member States' economies.

For the EU IT industry, VIS with biometrics would provide a greater stimulus, as there would be a need for high quality technical equipment to take, store, process and transmit personal data between national systems and the central part of the VIS. Consular posts, border check authorities, police and immigration authorities would have access to the VIS, which would require suitable computer terminals with high level of security and capacity to access, enter and update personal data (including biometrics). Data communication capacity and quality in the consular posts will also have to be improved.

For carriers, VIS with biometrics would have a greater, albeit mixed, impact than VIS without biometrics. VIS with biometrics should markedly reduce travel documents and visa fraud. Carriers might expect that fewer people would travel on false documentation, thus reducing the burden and cost for the carrier. On the other hand, biometric data in the VIS would enable checks to be made at the border crossing points as to whether the person travelling with a visa is the same person for whom the visa has been issued. In this way it may be expected that the rate of identification of persons trying to enter the external border illegally will increase. In such a scenario, carriers would be faced with a higher number of people to be returned to their original destination, with attendant other costs such as detention costs and, possibly, carrier liability charges.

5.4 Factors that could maximise benefits and minimise costs of policy option 4 'VIS with biometrics'

There are a number of factors which, if implemented, would maximise benefits and minimise costs of policy options:

- Joint visa issuing arrangements in some third countries would facilitate the technical implementation of visa information exchange systems. The existence of some joint visa issuing posts would mean that VIS with biometrics would be rolled out into one such post in a third country, rather than the current number of consular posts. This could result in a major saving in implementation costs. The installation of VIS with biometrics in one physical location in a third country could also mean better security and control over access to the system. However, as indicated elsewhere in this study, it would not be possible to implement such arrangements in locations in which very large numbers of applications are made.
- An independent body for supervising compliance with data protection requirements might monitor whether the use of personal data within the VIS meets EC data protection requirements. It would also consider and action complaints by visa applicants on misuse of their personal data within the VIS.
- Requirement for EU citizens to give biometric data to obtain EU passports would increase the social acceptability of the use of biometric data in official

databases. This would also reduce the retaliation risk by third countries as the EU could counteract the charge of treating third country nationals under visa obligation differently from its own nationals.

5.5 Which categories of personal data should be included in the VIS? Should the personal data of EU citizens and companies issuing visa invitations be included in the VIS?

In addition to the cost-benefit analysis of the two policy options, there are also a number of parameters which will impact on the effectiveness of the two policy options, as measured against the political objectives for a visa information exchange system.

It is suggested that, as a minimum, the data should include: full names, date and place of birth, sex, nationality, marital status, home address, occupation, purpose of application, address(es) to be visited in the Schengen territory, name and address of host(s)/sponsor(s) and/or any other person issuing an invitation, and details of previous applications.

The current Schengen visa application form contains nearly 50 categories of personal data, providing detailed information about the visa applicant. Personal data on visa applications is generally collected for several purposes:

- Proving the identity of the visa applicant;
- Certifying the official documents of visa applicant (details of passport);
- Establishing the validity of the visa application (destination, purpose and dates of travel, proof of invitation, proof of financial ability to pay travel costs).

Data protection considerations are explored in more detail in the Annex 3 to the report.

The inclusion of all the personal data categories, currently contained in the Schengen visa application form, would have the following impacts on achieving the political and operational objectives:

- Reductions in visa fraud and visa shopping.

Generally, the more personal data obtained about the visa applicant, the easier it is to establish his/her credentials and the validity of the visa application. From this perspective, the inclusion of all personal data categories would facilitate the identification by consular authorities of fraudulent visa applications (just as in the current situation).

Visa shopping would be affected to a greater extent by the inclusion of all personal data categories in the VIS. If the person uses the same identity to re-apply for the Schengen visa after visa refusal, the consular authorities in another Member State would have automatic access to all the personal data about the visa applicant from his previous application.

- Increased efficiency of border checks.

The main purpose of border checks, in cases in which a visa is held, is to ascertain that the traveller is the same person for whom the visa was issued, that the visa and travel document has not been fraudulently altered, that there has been no material change of circumstances since issue of the visa, and that the traveller fulfils the requirements for entry into the territory of Schengen states. For these purposes, border

checks would be facilitated by border guards having access to all the categories of an applicant's personal data on the VIS.

- Reductions in illegal migration.

The impact on identifying undocumented migrants would be felt only in cases where they had made their visa application in their true identity. In such cases, access to personal data to identify the person and official documents which he had when applying for a visa would help to identify the undocumented migrant and facilitate the removal process of such a person.

One means of entering illegally is to make false representations to the border guard about the length and purpose of one's stay. In general terms, possession of a valid visa should facilitate the passage through the border control. However, where there is reason to examine closely the holder of a visa, having full information available about the visa application enhances the border guard's ability to test the veracity and consistency of statements made at the border.

In addition, if a person found within a Member State is shown to have entered or remained illegally, but has no valid travel documents, the ability of the control authorities to identify, and document him/her for removal, will be enhanced by having as full details as possible of any visa application made.

- Contributions to internal security including the fight against terrorism.

The ability to identify major criminals and terrorists by using the personal data from the application form would arise, of course, only in cases where such persons:

  - come from countries whose citizens require visa to enter the territory of Schengen states; and
  - use their true (or other known) identity when applying for a visa.

The sophistication of organised criminals and terrorist networks suggests that such cases are extremely unlikely. Therefore, the impact of access to personal data categories on internal security and terrorism would be minimal. In addition, terrorists and major criminals may enter clandestinely or by using false documents showing they do not require a visa. Again, the question of information from a visa application does not arise.

- Efficiencies for bona fide travellers

Retention of all the personal data categories on the VIS would be beneficial to bona fide travellers. For frequent travellers, the storage of their personal data would facilitate subsequent applications, as consular authorities would be able to check and confirm the personal data from the previous applications. Those categories of data establishing identity (including names, date of birth, nationality and purpose of journey) would be of most value in such cases.

For bona fide travellers who have lost their travel document whilst in the territory of Schengen states, the storage of their personal data would facilitate their identification and documentation. It may be envisaged that data categories proving the identity of the traveller (including names, date of birth and nationality) would be most beneficial for such purpose of identification.

One group of frequent travellers are professional drivers in the land transport sector. The identification of such a person through biometric data would make their visa applications easier, as less checking would be needed to confirm the identity of the driver. Their record of complying with visa and immigration requirements would be securely established in the system, and the authorities could fully rely on the data provided, which would help the professional drivers to get consecutive visas and cross borders with ease. In VIS without biometrics it would be difficult to establish the connection between an individual's past history and the person concerned. In addition, if the EU is considering giving the professional drivers longer multiple entry visas, VIS with biometrics would be needed.

- Inclusion of data on EU persons issuing invitations

Inclusion of such data in the VIS would help to identify those persons, companies and organisations which issue fraudulent invitations[82] for third country nationals requiring a visa to enter the Schengen territory. This would be important information in the fight against visa fraud, which is called for in the Article 27 of the 1985 Schengen convention.[83]

Knowing that a EU citizen, company or organisation made a fraudulent invitation for a third country national in the past, or even that a particular person or other organisation has figured regularly in doubtful cases, without some reasonable explanation, would alert the consular authorities to the possibility of fraud. It might suggest, in appropriate cases, that the individual, company or organisation was involved in the attempted facilitation of illegal migrants.

The identification of fraudulent (or doubtful) sponsors is an issue for the Member State in which the sponsor is resident, since the third country national would apply for the visa of this Member State. In principle, therefore, information about sponsors should normally need to be stored in the national systems only, and not on the central part of the VIS.[84] However, given the international nature of terrorism, major crime and illegal migration, there may cases in which an individual, company or other organisation is identified as having been involved in doubtful cases dealt with by more than one participating Member State. In such cases, it would be important for the details of the individual, company or other organisation to be available to consular staff in all participating states, and accordingly for relevant data to be stored on the central records of VIS.

Against such beneficial impacts on reducing visa fraud, one must bear in mind that the storage of personal data on EU citizens should be necessary and proportional and would have to comply with the current EU data protection legislation. The effect of this is that EU citizens would have to be informed about the storage of their personal data on the VIS, their consent would have to be obtained to store their personal data, and

[82] In this context "invitation" is intended to include a personal invitation, for example from a friend or relative, a letter of sponsorship, a letter or other document from an educational institution, confirming acceptance for a course of studies, and a letter or other document purporting to show that a person was expected, to conduct business with a company based in the EU.

[83] Article 27 calls on contracting parties to impose appropriate penalties on persons who for financial gain assist alien to enter or reside within the territory of one of the Contracting Parties in breach of that Contracting Party's laws on the entry and residence of aliens.

[84] The architecture of the system has been analysed in detail in the VIS Feasibility Study.

they would have to have a right of access to their personal data (that is, unless national laws stipulate that there is no necessity to obtain the consent of the EU citizen for reasons, for example, of internal security).

5.6 What would be the impact of including scanned documents in the VIS?

If the documents supporting a visa application are scanned, this would facilitate the return procedures. A major obstacle to effective return procedures is the lack of necessary travel documents for illegal migrants apprehended. Countries of origin often delay or deny the issue of return travel documents, because of declared uncertainties over the identity and nationality of the person concerned. The consequence of this is lengthy and expensive procedures of identification, often involving detention, and the need to present the person who is to be removed to his/her Embassy or consular authorities, and/or conducting language or dialect analysis. Having not only the alphanumeric data on the travel document (such as its number), but also a scanned copy of a travel document produced at the time of the visa application would do a great deal to persuade the illegal migrant's authorities to issue a replacement travel document without delay. A paper copy of supported documents could be kept available in the consular office and therefore would have not to be stored in the system.

On the negative side, the scanning of documents would use a great deal of capacity in the system, and generate a lot of work for the consular officers. For all visa applicants, who are estimated as 20 million a year, an extra operation would be needed at the consular post. This would have significant resource implications and scanned documents would only be used in limited cases. Eurostat statistics show that only around 350,000 people, illegally present in the EU territory, are apprehended annually, many of whom do not have a document showing identity and nationality. Therefore, in more than 98% of cases the scanned documents would never be used.

The inclusion of scanned documents would also carry an additional financial cost.[85] A possible solution would be to provide for documents to be scanned selectively, in accordance with agreed instructions. This might apply, for example, when there were doubts about an applicant's bona fides, but insufficiently so to refuse the application; or in the case of nationalities or groups known to be particularly difficult to document after apprehension as illegal migrants. Such documents would then be available, on request, and could be received off line. If the authorities of the Member State required copies of travel documents for returning an illegal migrant, they could use the VIS to locate the consular post that stored the scanned documents, and ask for the documents to faxed or mailed to them, if available. Such a selective approach to the scanning of documents could be a more proportionate response to the issue. In addition, it should be underlined that the basic alphanumeric data of travel documents, such as the type and number of the passport, the authority which issued it, and the date of issue and expiry, would be available in the VIS without scanning the document.

[85] DG JHA estimates that for the Community budget the inclusion of scanned documents will add €1 million to the annual operating costs.

5.7 What should be the length of retention period of data on the VIS?

The Council conclusions for the VIS envisage the storage of personal data in the central system of VIS for a period of "at least five years" for the purpose of on-line consultation.[86]

There are a number of options regarding the length of such retention period:

- Storage of data for the time period of visa validity, i.e. period authorised in the visa;
- Storage of data for 5 years;
- Storage of data for another period.

The precise choice of a retention period should be linked to the purposes of the data processing, as stipulated in the European data protection legislation. If there is a justified legitimate reason for keeping personal data for longer periods, this would be in line with the data protection requirements.

Measured against objectives of the visa information system, the following impacts of the choices for the retention period could be noted.

- If personal data should be retained only for the period of the visa's validity, the contribution to the reduction of visa shopping and fraud, better border checks, to fight against illegal migration, terrorism and organised crime would be very limited. This retention period would not allow any speeding up of subsequent applications for regular travellers, as their record would only be stored for the period for which the visa is valid. In addition, it would be unlikely that such a period of validity would assist in the documentation of illegal migrants, who, at some stage had applied for a visa.
- Should a five-year period be chosen for the retention period of personal data, the contribution to the reduction of visa shopping and fraud, better border checks, to the fight against illegal migration, terrorism and organised crime would extend for the period of time chosen. Advantages for regular travellers would also extend for the period of time their personal data is stored on the VIS.

At present, there is no universal practice on storing data in such systems. In current databases, the retention period differs substantially. In the Eurodac database, the fingerprints of asylum applicants are stored for ten years.[87] Common Consular Instructions recommend keeping visa applications for at least one year where the visa has been issued and at least five years where the visa has been refused.[88] In practice,

[86] Council Conclusions on the development of the Visa Information System, 19 February 2004.

[87] Regulation 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, 11 December 2000.

[88] Part VII, point 2, Common Consular Instructions on visas for the diplomatic missions and consular posts, OJ C310, Volume 46, 19 December 2003.

Member States have differing arrangements for keeping visa records, sometimes over and above the requirements of Common Consular Instructions.[89]

- If data is stored for another period to contribute to the reduction of visa shopping and fraud, better border checks, to fight against illegal migration, terrorism and organised crime the storage of personal data would need to continue for as long as a traveller is likely to re-apply for a visa. In practice, this could in many cases entail the indeterminate storage of their personal data for regular travellers. For regular travellers, the indeterminate storage of their personal data from past visa applications would have an advantage of having all their past visa applications available to all Member State consular authorities. However, the indeterminate storage of personal data of all visa applicants would have an extreme negative impact on privacy and data protection of visa applicants. Such a system would also be extremely expensive to maintain and keep secure. It must also be kept in mind that the possibility of finding the data relating to a specific person in a biometric database would decrease in proportion to the increase in the volume of data that the database contained.

5.8 Which authorities should have access to personal data contained in the VIS?

In view of data protection and proportionality requirements, the access to VIS data should be determined by specified, explicit and legitimate purposes for which the data should be used according to the objectives of the VIS.

The impact (as measured against the objectives of a visa information exchange system) of providing access to data stored in the VIS would be the following:

- For the purposes examining the visa application including the consular cooperation and the consultation of central national authorities, access should be given to consular authorities including the central authorities and border crossing points issuing visas.
- To help to reduce visa application fraud and visa shopping, granting access to VIS data to the consular authorities would be sufficient. It is consular authorities that are primarily involved in the visa issuing process and are in the position to detect visa application fraud and visa shopping. Granting access to VIS data to the consular authorities and border control authorities would be sufficient to help to reduce travel document fraud.
- To increase the efficiency of border checks, granting access to VIS data for border control authorities would be sufficient.
- For the purposes to contribute to the fight against illegal immigration, including identification and return of illegal immigrants, and to facilitate the application of the Dublin II Regulation, granting access to VIS data for immigration authorities and other competent authorities would be sufficient.
- For the purposes to contribute to the prevention of threats to internal security including the fight against terrorism, access to VIS data would be sufficient for consular authorities, border control authorities and immigration authorities,

[89] For example, France keeps the records of visas issued for 2 years, and of visas refused for 10 years. See Guidelines for the introduction of a common system for an exchange of visa data, 9615/02, Visa 92, Comix 386, 5 June 2002.

according to their horizontal objective to contribute to the prevention of threats to internal security of any of the Member States. In particular by the outcome of the consultation between national authorities, VIS data and the checking of the SIS alert list for the purposes of refusing entry would enable consular authorities to detect when a known terrorist or organised criminal applies for a Schengen visa, as well as enabling border control authorities to recognise a known terrorist or organised criminal when they try to enter the territory of Schengen states. Similarly, if a known terrorist or major criminal has applied for a visa, access to VIS would enable immigration or other relevant authorities identify him/her, if apprehended in the territory of Schengen states, or indeed (in the case of immigration authorities) if an application to remain is made. In general, VIS data would not help to identify terrorists or organised criminals if they are not already known as such to authorities, though being able to "plot" a suspected person's movements by reference to a visa application(s) could be of value to the relevant authorities.

- For the purposes to facilitate the travel of bona fide travellers and regular travellers, in particular, access to VIS data for consular authorities and border checkpoints would be sufficient. This is because consular authorities would speed up the processing and checking of regular travellers' applications for a visa.

It appears, therefore, that the achievement of the objectives set for a visa information system does not require access to VIS data for a wider range of authorities. Indeed, granting access to VIS data to a wide range of authorities could lead to a situation where, due to the number of access points, it is problematic to ensure security and consistent use of the system data. There might, however, need to be coordinating points through which requests for access could be routed, in the case of authorities without direct visa, border control and immigration control responsibilities, but with a legitimate need for particular information.

However, for the access to the VIS data, there is not only the need to define the competent authorities by the specific purposes, but for each of these purposes it has to be specified:

- The categories of data to which the competent authorities should have access for the specific purposes;
- The search criteria, which will indicate that there are data stored on the applicant in the VIS.

It should also be ensured that access to the data should be reserved exclusively to duly authorised staff of the competent authorities and limited to the extent the data are required for these purposes

6 PLAN FOR MONITORING AND EVALUATION

The effective monitoring of the VIS requires evaluation at regular intervals. For these purposes, it is necessary that systems be in place to monitor the functioning of the VIS against objectives, in terms of outputs, cost-effectiveness and quality of service. It is recommended that in regular intervals like two years a report on the technical functioning of the VIS should be submitted to the European Parliament and the Council. This report should include information on the performance of the VIS against quantitative indicators predefined by the Commission. Moreover, in further regular intervals like four years, an overall evaluation of the VIS should be produced, including examining results achieved against objectives and assessing the continuing validity of the underlying rationale and any implications of future options.

As elaborated in Section 1, the overarching problem in the current situation is the lack of exchange of visa application information between the consular authorities of Member States. This jeopardises a fully effective implementation of common visa policy, which when successful should also help to achieve the following objectives:

- Reduce visa application fraud, visa shopping and travel document fraud;
- Facilitate the application of the Dublin II Regulation;
- Contribute to more efficient border checks;
- Contribute to the fight against illegal migration;
- Contribute to the fight against terrorism and increasing internal security;
- Increase advantages for bona fide and regular travellers from third countries.

In the recent work for the Commission on the policy evaluation framework,[90] EPEC has identified the following characteristics of a 'good' indicator:

- The indicator is closely linked to a policy goal, objective and/or target. (Indeed, indicators are most helpful when objectives have been specified in terms of targets or milestones that apply the definition of the indicator).
- It is measured regularly. It is helpful to have time series information where the precise indicator definitions have been applied consistently. Ideally data should be available prior to the adoption or implementation of the policy and legislation. However, policy initiatives often themselves call for new data to be collected.
- It is measured on an independent basis. It is preferable that information is collected by agencies not directly responsible for the policy or legislation.
- The measurement is based on reliable data.

[90] Preparatory Study of Policies and Legislation – Development of an Analytical Framework, http://www.europa.eu.int/comm/dgs/justice_home/coordination/evaluation/epec_final_report_en.pdf.

On the basis of these observations, the following indicators could be applied to measure performance of a visa information system. Detailed indicators and targets would need to be developed, in order to gauge the success of a VIS, with or without biometrics. Table 6.1 identifies the types of problems that need to be monitored, potential indicators, data sources, potential targets and milestones and the rationale for the suggestions made.

In addition, some contextual indicators should be monitored in the course of implementation of VIS, for example:

- Number of visa applications;
- Main source countries of visa applications;
- Any signs of retaliation to the implementation of the VIS;
- Any economic consequences of the implementation of the VIS, such as travel volumes (to and from) third countries into the EU, both leisure and business travel.

Table 6.1. Potential success indicators and targets for a visa information exchange system

Problem	Potential indicator	Data source	Potential targets and milestones	Rationale
Lack of exchange of visa application information	Average time taken to process an application	Data from Member States	Baseline data required	The aim is to process applications quick and cheap
	Reductions in costs of administering a visa system	Data from Member States	Baseline data required	Aim is to process applications quick and cheap
	System availability rate	VIS	99.9%	System should be available to consular authorities 24 hours a day, 7 days a week.
	Number of mistakes in the system (e.g. false identification)	Data from Member States	<0.1%	System should provide reliable means of identification and verification of visa applicants
	Number of entries on the system	VIS	20 million in 2007	To show whether consular authorities would make full use of the system
Visa application fraud, visa shopping and travel document fraud	Numbers of visas refused, annulled, revoked indicating the standard grounds	VIS	Baseline data required	This is one of the main objectives of VIS.
	Numbers of fraudulent travel document identified; category (e.g. counterfeit, altered personal particulars)	VIS	Baseline data required	This is one of the main objectives of VIS.
	Number of repeat applications in the 12 month period after a visa refusal	VIS	Baseline unknown.	Decisions about visa applicants should be better with VIS
Illegal migration	Number of illegal migrants apprehended, documented and removed (could also include details of forms of illegal migration, like clandestine entry, overstaying)	Data from Member States	Baseline 360,000 apprehended in 2001.	Decisions about undocumented illegal migrants should be better with VIS
	Number of visa overstayers detected	Data from Member States	No baseline	Detections of visa overstayers should be better with VIS

Contributions to internal security	Numbers of persons regarded as a threat to internal security on national 'watch lists' detected when applying for a visa and crossing external borders	Data from Member States	No baseline	More terrorists and organised criminals should be detected
Bona fide travellers	Average application processing time	Data from Member States	Baseline data required	Applications should be processed quicker and more efficiently
	Number of objections by visa applicants	Data from Member States	No baseline	This would show compliance with data protection requirements and customer satisfaction rate
	Number of appeals by visa applicants	Data from Member States	No baseline	This would show compliance with data protection requirements and customer satisfaction rate

The main problems caused by a lack of efficient, effective exchanges of information are:

- Failure to recognise trends, for example particular forms of deception practised;
- The absence of consistent statistical material, resulting in an inability to submit necessary monitoring material, for example on the different types of fraudulent documents identified;
- The failure to exchange information on issues such as the safety (or otherwise) in countries from which asylum applicants come;
- Failure to exchange information on routes used by illegal migrants, and organisations assisting them, and on apparently legitimate organisations, that might be assisting people to enter fraudulently.

A VIS, with or without biometrics, would help Member States to collect, assess, and disseminate relevant information about such problems. These might include:

- Information on visas refused, annulled or revoked for different grounds, like failure of a valid travel document, no submission of supporting documents, alert on the applicant or a threat to internal security;
- Organisations and individuals found to have facilitated or sponsored intending illegal migrants;
- Information on 'visa shopping' by the dates and the grounds of previous visas refused;
- Statistics regarding categories of application, and breakdown by nationality of grants/refusals.

ANNEX 1: US VISIT SYSTEM

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is an elaborate and integrated electronic programme intended to improve US capability to collect information about foreign nationals who travel to the United States, as well as control the pre-entry, entry, status and exit of these travellers and verify their identity. In this respect it has much wider objectives and coverage than the proposed VIS of the EU. The aims of the US-VISIT are to ensure border security, enforce immigration laws and facilitate legitimate travels.

The system is envisaged to work as a continuum of security measures. It begins at the US consular offices issuing visas where biometrics are collected to determine whether the applicant is on a database of known or suspected criminals or terrorists. When the visitor comes to the US border, the same biometrics are used to verify that the person at the entry point is the same person who received the visa, or to see whether there is new information about any involvement in terrorism or crime. Foreign visitors exiting the United States will be required to confirm their departure at the exit points. This should demonstrate their compliance with immigration requirements and facilitate their future travels. People who overstay their visas would also be identified in this part of the system.

If a person refuses to provide fingerprints or be photographed, he/she is not permitted to enter the country. The US-VISIT programme applies to visitors travelling to the United States on visas. It does not collect biometrics from travellers coming through the Visa Waiver Programme, which includes most of the EU Member States.

Main issues raised so far regarding the US-VISIT:

1. Burdens on legitimate travellers. US government announced that trials have shown that on average 15 seconds are added to entry procedures when biometrics are taken. However, with large volumes of traffic (30 million people crossing with visas in 2003), it can be reasonably expected that the system will slow down the processing times at the border.
2. Implementation issues – infrastructure and facility needs at the border. Entry ports themselves face considerable challenges in the creation of an automated alien tracking system due to their location, infrastructure, geography and traffic volume. There is a real potential to slow down the flow of traffic at points of entry and demands for dedicated space to record data for US-VISIT. The current infrastructure is not sufficient to accommodate the demands of the US-VISIT.[91]
3. Adequate protection of privacy. In contrast to the EU data protection legislation, US does not provide for protection of processing of personal data of third country nationals. Also, in the cases of false rejections or other system mistakes, persons are not informed of the reasons for the rejection, and do not have any means by which they might assert their own point of view before any decision is taken.

[91] US VISIT, Congressional Research Service Report for US Congress, 18 February 2004, RL32234.

- The US-VISIT has a privacy officer whose duty is to ensure that the privacy of visitors is respected and to respond to individual concerns. However, it has been questioned that the privacy officer has great discretion to respond to complaints.

- There are no specific enforceable procedures for redress if a visitor is denied entry to the United States as a result of US-VISIT, wants to review the information US-VISIT contain about him, or wants to correct inaccurate, irrelevant, outdated or incomplete information in the system. Official redress policy seems to do little to secure these rights.

- There has been sharp criticism from the American Civil Liberties Union and immigration rights groups over how the personal data will be protected under the US-VISIT and how the government will ensure that the programme does not unfairly target innocent people for deportation or denied entry.

4. The system has been accused of being defined imprecisely how it will work, who will be covered, what technologies will be deployed, and how much will it cost in total. The General Accounting Office called it a very risky endeavour because of management and financial concerns. The scope of the use of the system information, for example, is not clear. The Attorney General possesses broad discretionary powers to allow law enforcement agencies access to the US-VISIT.
5. The decision to hire a private contractor was criticised because instead of defining precisely the requirements for the US-VISIT, the government left it to the companies to define their vision of how to track foreign visitors. Given that the price tag for the US-VISIT could come to $15 billion, the government was expected to give more direction and leadership on the development of the US-VISIT.
6. Concern over the 'mission creep' and potential to overstep the legal uses of the information contained in the US-VISIT. The vast amount of information contained within the system makes it an ideal research tool for many purposes. There are many reasons why law enforcement agencies may want to use the system for other purposes than defined in the law.

Tracking the entry and exit of most foreign nationals at US borders is no small undertaking, as in 2003 there were over 427 million people arriving at the US entry points, of which 62% were foreign nationals. In 2002, around 30 million people arrived at US borders with regular visas.

The system was deployed at 115 airports and 15 major seaports on 5 January 2004, and the 50 highest volume land ports of entry will be phased in by 31 December 2004, with all remaining ports of entry integrated by 31 December 2005. The programme received $380 million for the fiscal year 2003 and was given $330 million for the fiscal year 2004. A private company Accenture and partners was awarded the contract to build and operate US-VISIT in May 2004. The contract is worth estimated $10 billion over the next 5 years.

US-VISIT collects personal information on foreign visitors and also scans, collects and uses biometric identifiers of visitors to the United States. An inkless fingerprinting system captures left and right index fingerprints and a digital photograph is taken. Personal information includes complete name, date of birth, citizenship, sex, passport

number and country of issuance, country of residence, United States visa number, date, place of issuance, alien registration number, address while in the United States, and any other information deemed suitable for enforcement of the immigration laws and safety and national security.

US-VISIT is expected to integrate over 20 existing US national systems which are concerned with collecting information about foreign visitors. In this respect the integration of visa systems in the existing EU Member States could be seen as a similar task. However, it is worth mentioning that in the US, a number of databases with different operational purposes are being integrated, whereas in the EU, it would be a case of substituting existing arrangements where visa application data is kept at the national level, with a system of exchange of visa application data between Member States.

ANNEX 2: COMMENTS ON DETAILED VIS BIOMETRIC OPTIONS

1. Storage of biometric data – on the VIS/only on the visa/in the VIS and on the visa

It can expected that biometrics would be used in the operation of the VIS in the following ways (as identified in the VIS feasibility study).

VIS business process	What happens?	Should biometrics be stored on VIS?	Should biometrics be stored on visa?
Visa issuing without previous registration	A negative identification is performed each time a visa applicant is not in possession of a previously issued visa. This is done to avoid enrolling the same person under two identities and visa histories. A one to many comparison is launched to check if a person has already applied for a visa under another identity.	Essential	Not necessary
Visa issuing with previous registration	A one to one comparison is used to confirm that the person is still the same person as the one who has previously applied for a visa	Essential	Advantageous
Visa and traveller identification	Verification of visa holders is performed at the external border checkpoints, police and immigration departments of Member States. The verification, one to one comparison, should prove that the visa carrier is the same person as the visa holder.	Essential	Advantageous, although dependant on the availability of equipment to check biometric data in visas
Person identification	Positive identifications are performed by police and immigration officers possibly after failed verification or if the person is totally unknown.	Essential	Probably not necessary, as majority of persons in this process will be undocumented illegals

These preliminary considerations indicate that the storage of biometric data should be confined to the VIS as the storage of biometric data on visas would be of some benefit in the process of visa and traveller identification primarily at entry points to the EU. However, for data protection purposes biometric data should not be stored in a database but rather only in an object exclusively available to the user.[92]

2. Locations to take biometric data – consular posts or travel agencies

The decision on which locations are suitable for taking the biometric data will have huge resource implications for travellers and travel agencies. At the moment, there are arrangements under which travellers can also submit their applications for a visa via approved travel agencies, who then forward the application to the consular post of a Member State. With the introduction of mandatory taking of the biometric data, travel agencies would need to spend substantial resources to ensure the right equipment, premises and security for taking of biometric data. However, in any event, given the sensitivities of travel agencies collecting biometric data, there are real doubts whether such arrangements could be allowed to continue. Therefore, the only suitable locations to take biometric data would appear to be consular posts. In this case, travellers applying for a visa would have to come to a consular post in person to give biometric data. Unless arrangements could be made for biometric data to be collected by properly authorised and trained staff locally, this would cost visa applicants a lot of time, sometimes involving travelling huge distances to the capital cities of big countries like, for example, Russia, and thus constitute a substantial burden on bona fide travellers.

The only viable alternative would be to allow biometric data to be taken at approved centres, for example a local Immigration Office, but then there would be resource implications (additional equipment would have to be installed), and staff would have to be trained.

3. Photographs – digitised photograph or original photograph taken with a digital camera

The decision for the applicant to have an original photograph taken with a digital camera would also entail that the traveller has to come to the consular post in person. Again, this would cost them a lot of time, sometimes involving travelling huge distances to the capital cities of big countries like, for example, Russia, and thus constitute a substantial burden on bona fide travellers - unless proper arrangements could be made for local staff to handle this.

The decision to have a digitised photograph would enable travellers to submit their photos accompanying their visa applications via intermediaries like travel agencies. The impact of the decision on locations to take biometric data has been considered in the section above. Should a decision to have digitised photographs taken in the travel agencies be made, this would reduce the opportunity costs for travelling time and cost for visa applicants.

4. Storage of 2 or 10 fingerprints

The question on the number of fingerprints to be stored is largely a choice between accuracy and cost. The more fingerprints a system will hold, the more accurate it will be and the level of errors would remain lower. An increased number of fingers

[92] This is the view adopted by the Article 29 Working Party on Data Protection, see Working document on biometrics, p. 6.

results in higher accuracy of the system. However, development and annual maintenance of the system, which uses ten fingerprints, is costlier than a system where only two fingerprints are used. The use of ten fingerprints also enhances the size of the system, which carries a cost as well.

VIS feasibility study recommended using ten fingerprints, because such an approach is more reliable, reduces the risk of insufficient accuracy, is easier to capture than specific fingers and will allow background checks against SIS and other databases.[93] It also noted that it would require less supervision from the consular staff to take ten fingerprints rather than various specific fingers, and that even if some fingers are temporarily damaged and therefore not available, remaining fingers can still be used for comparison.

Proposals for making visas more secure and less prone to fraud envisage that the number of fingerprint images stored on the visa should be limited to two.[94] This is because they will be used only for verification purposes (one-to-one checks) and no searches in the VIS would be performed. The proposal also envisages an opportunity to review the number of fingerprints should the failure rate for verification be too high.

US-VISIT system uses left and right index fingers for the identification of travellers in the entry-exit implemented in the US. It is also worth noting that thumbs and the indexes are the fingers with the most informative content. So the storage of two fingerprints was considered to be sufficient for the purposes of entry-exit system. The two fingerprint IDENT system that US authorities introduced on the southern US border has proved resilient, sorting through 6 million records on a one-to-many basis to perform criminal checks. Recent National Institute of Standards and Technology tests showed that it has a 95.5% accuracy rate and resulted in a false positive 0.05% of the time in one-to-many searches.[95] For this reason, it was selected for the initial deployment phase of US-VISIT. However, some concerns surfaced about its scalability, i.e. how many could be enrolled before the system would finally cease to be accurate. However, it was viewed as the best option for rapid implementation. The two fingerprint system is almost certain to suffer a serious drop in performance once the database gets really large.

[93] VIS feasibility study, p. 45.

[94] Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas and a Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third country nationals, COM(2003)558 final, 24 September 2003.

[95] Fingerprint Vendor Technology Evaluation 2003: Summary of results and analysis report, NISTIR 7123, June 2004, p. 5.

ANNEX 3: DATA PROTECTION CONSIDERATIONS RELEVANT TO THE VISA INFORMATION SYSTEM

Introduction

Public and private processors of personal data are bound by the protection provisions, enshrined in the Charter of Fundamental Rights (Article 8), and in the EC data protection legislation.

The main legislative EC instruments regulating the personal data protection are:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. However, this Regulation applies only to Controllers for the processing of personal data by on behalf of Community institutions and bodies.

The EC data protection legislation is based around the notions of *rights* accorded to the persons (or 'data subjects'), and the *obligations* placed under data controllers and their related processors to maintain a high transparency and efficient controls over the processing of personal data.[96] As the legislative proposal on the VIS (with or without biometrics) is a first pillar instrument, the EC data protection legislation would apply in full in the implementation of VIS.

1. Application of general principles

The implications of applying the data protection principles in the implementation of Policy option 3 'VIS without biometrics' and Policy option 4 'VIS with biometrics' could be described as follows:

1. Regarding the principles relating to data quality and lawfulness of processing:
   - "Personal data must be processed fairly and lawfully".[97] This means that the processing must take place in accordance with the law and that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the

[96] 'Controller' is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

'Processor' is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. Article 2 of Directive 95/46/EC.

[97] Article 4(a) of Regulation 45/2001 and Article 6(a) of Directive 95/46/EC.

protection of health or morals, or for the protection of the rights and freedoms of others"[98].

- "Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".[99] It could be considered that the primary processing of personal data in the VIS is to facilitate the implementation of common EU visa policy by improving exchanges between the consular authorities to make better decisions about visa applications. Other purposes of the VIS, such as contributing to the fight against illegal migration or contributing to internal security relate to VIS insofar as they are applicable to the implementation of common visa policy. The requirement for nationals of designated countries to produce valid visas on arrival are an integral part of the arrangements under which third country nationals may enter a Schengen State. Any overstay of a permission to enter or remain is considered illegal. Therefore, information to identify an overstayer who entered the territory with a valid visa is of direct relevance in the context of fighting illegal migration.
- Examination of a visa application allows consular authorities to contribute to the prevention of threats to internal security, by making appropriate enquiries as to whether a visa applicant constitutes a threat to internal security, by for example, having a criminal record, being involved with acts of terrorism or association with others who are so involved. For this purposes, national alerts will be checked in the framework of the consultation between central authorities, including background checks on national databases and alert list.

In the light of the above, transfer of personal data from VIS users to other authorities should be governed by the needs and purposes of VIS and the implementation of common visa policy. In particular, the access rights to the VIS needs to be drawn up in the legislative proposal.

- "Processing of data must be adequate, relevant and not excessive to the purposes for which they are collected and/or further processed".[100]

  - "Adequate" processing of data is commensurate with the objectives of VIS and scale of the problems in the current situation (as outlined above?). In this respect, there is a certain dilemma in that improvements in the current situation would be greater if personal data are retained on VIS for longer time periods.

  - The question of "relevance" relates to the question of which personal data categories from Schengen visa application form are relevant for the determined purposes. Current Schengen visa application form contains 48 categories of personal data. An assessment is needed of which data are necessary to fulfil these purposes, in particular to which extent only the categories of most relevance for the identification of person should be stored on the VIS, such as name, date of birth, sex, birth date and place, nationality, details of travel document etc. Assessment is also needed for which

[98] Cf. Article 8 of the ECHR.

[99] Article 4(b) of Regulation 45/2001 and Article 6(b) of Directive 95/46/EC.

[100] Article 4(c) of Regulation 45/2001 and Article 6(c) of Directive 95/46/EC.

categories for applications further information is needed, e.g. for the purposes of consultation between central authorities. There is also an issue of whether the data of EU citizens issuing invitations for third country nationals (the so-called sponsors) should be stored in the VIS (this is considered in detail in section 5.5.1).

- The principle of "not excessive", relates to the amount of data that might be processed. This would mean that the determination is needed which of the data stored in the VIS should be used for the specific purposes of the VIS.

- "Personal data must be accurate and, where necessary, kept up to date".[101] It can anticipated that there would be a need to correct data stored on the VIS, either because of human mistakes when entering the data or changes in person's circumstances, e.g. a change of name. In this respect, it is required by law that visa applicants have the opportunity to access their data and get their records amended, in accordance with laws and procedures of Member States. For this purpose, Schengen visa application form could be amended to inform visa applicants of such a right.

- "Personal data must be kept in a form which permits identification for no longer than necessary for the purposes for which data were collected".[102] In this context the issue of retention period is important. The proportionality of data retention period has been considered in the section 6.5.

2. Section 5 of Regulation 45/2001 and sections 5 and 7 of the Directive 95/46/EC (rights of the data subject). This would entail a provision for the rights of the data subject to access personal data contained in the VIS, and right to object to data controller and right to appeal to independent national supervisory authority.

3. Section 7 of Regulation 45/2001 and section 8 of Directive 95/46/EC (confidentiality and security of processing). Appropriate technical and organisational measures should be taken against unauthorised use and unlawful processing. For that purpose, it would be necessary to foresee technical installation that would prevent unauthorised access.

Monitoring should ensure that these principles are applied correctly in the implementation of VIS, fundamental rights of persons as regards their rights concerning processing of their personal data should be secure.

As long as data protection legislation is applied correctly, and the proportionality of the use of biometric data in the system is proven, the inclusion of biometric data does not require additional data protection measures. In other words, regardless of whether biometric data is included or not, a visa information exchange system would have to comply fully with these data protection requirements[103].

---

[101] Article 4(d) of Regulation 45/2001 and Article 6(d) of Directive 95/46/EC.

[102] Article 4(e) of Regulation 45/2001 and Article 6(e) of Directive 95/46/EC.

[103] The first evaluation report on the implementation of data protection Directive 95/46/EC outlined three main issues in ensuring compliance: Under-resourced enforcement effort and supervisory authorities with a wide range of tasks, very patchy compliance by data controllers, low level of knowledge of their rights

In the course of this study, a number of specific issues regarding the data protection requirements of processing of personal data have arisen. They are considered in detail in sections below.

2. Transfer of VIS data to third parties

Transfer of data to the third countries or international organisations is a very sensitive issue. Any transfer of personal data to such third parties should be subject to additional safeguards to agree the suitability of such transfer. It can be envisaged that there will be a Community agreement on the additional safeguards before any such transfer of personal data from the VIS takes place.

Transfers of personal data to third countries and international organisations have to follow the following legal requirements: If the processing (= the transfer) is under Regulation (EC) 45/2001 Article 9 is applicable[104]. If the processing is under the Directive 95/46/EC implemented in national law chapter IV on the transfer of third country, containing Articles 25 and 26, is applicable.

In any case, EC data protection legislation requires for such transfer of personal data in particular that an adequate level of protection is ensured in the country of the recipient or within the recipient organisation. In the context of VIS, this would mean a transfer of personal information of very sensitive nature (even more so if biometric data is included). In this context, a main challenge for controllers of VIS would be to ensure that there is no purpose creep after the transfer of data to the third country or international organisation in question. It would therefore have to be ensured that the recipient country or organisation has laws and practical arrangements to guarantee the lawfulness and security of data processing and can prevent the misuse or unauthorised use of data. These laws and practices have to amount to being fully adequate and not only guarantee the security or prevent misuse. Given the impact on privacy, these arrangements will have to be very stringent.

3. Information required by the data subjects on the processing of their personal data

Visa applicants and other persons concerned by the processing of personal data in the VIS[105] must be informed that data processing is taking place and in all the cases they must be provided with the following information:[106]

- The identity of the data controller and of his representative.
- The purposes of the processing for which the data are intended.

---

among data subjects. However, this report is focussing on the private sector whereas the VIS will be operated and used by public authorities.

[104] For more information on article 9 transfers under the Regulation see: http://www.cc.cec/dataprotectionofficer/website/recommendations/DLegalClausesTransferOfPersonalDatamerged.doc.

[105] Such as EU citizens issuing invitations for visa applicants.

[106] Article 11, Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

- The recipients or categories of recipients of the data (consular posts, border check authorities, police and immigration authorities).
- Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply (it can be envisaged that the provision of personal data will be compulsory and the failure to comply will result in the rejection of visa application).
- The existence of the right of access to, and the right to rectify, the data concerning the visa applicant. However, it also must be kept in mind that the administrative burden of dealing with appeals and rectifications may primarily fall on the consular posts, which are bound to comply with data protection requirements.[107] The right to object with data controller and the right to lodge a claim and appeal to the national supervisory authority and the courts should also be specified.

This information could be provided to visa applicants on Schengen visa application form. The current application would have to be modified to take account all of these requirements. As far as persons issuing invitations or liable to pay the costs of living during the stay are concerned, this information could be provided in the respective forms to be signed by these person.

In addition, one could envisage that visa applicants could also be provided with the following information:

- The legal basis of the processing operation for which the data are intended (a reference could be made to the legal instrument establishing the VIS).
- The time limits for storing the data.
- The right to have recourse to the competent supervisory authorities.

However, the data subject's rights are subject to exemptions and restrictions. Directive 95/46/EC specifies that Member States can adopt legislative measures that restrict the data subject rights when such a restriction constitutes necessary measures to safeguard:

- National security;
- Defence;
- Public security;
- The prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

[107] It is difficult to estimate however the extent of this administrative burden of appeals and rectifications. The past experience from the application of data protection directive 95/46/EC suggests that majority of data controllers did not consider that responding to requests from individuals for access to their personal data involved an important effort. Most of the data controllers consulted either did not have figures available or received fewer than 10 requests during the year 2001 (First Report on the Implementation of the Data Protection Directive 95/46/EC), COM (2003) 265 Final, Brussels, 15 May 2003). However, the level of requests for access and rectification could be reasonably expected to be higher as the VIS would enable to make visa decisions on the basis of having biometric data.

- An important economic or financial interest of a Member State or of the EU, including monetary, budgetary and taxation matters;
- A monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases of public security, dealing with criminal offences, and important economic or financial interests;
- The protection of the data subject or of the rights and freedoms of others.[108]

Regulation 45/2001 also stipulates that if such restrictions are imposed, the data subject must be informed of the principal reasons such restrictions are enacted and of his/her right to have recourse to the European Data Protection Supervisor.

4. Background checks of VIS data against other databases

According to the Council Conclusions of 19 February 2004 on the development of the VIS, the technical functionalities of the VISION network for consulting the central authorities should be integrated into the VIS. This means that the VIS should not change the current system of consulting the central authorities on the basis of Article 17(2) of the Schengen Convention, including the background checks against national alert lists and data basis which are carried out according the national law of the Member States. Integrating the technical functionalities of the current VISION network would in principle imply no change from the current arrangements, based on Article 17(2) of the Schengen Convention and the Common Consular Instructions, and therefore no additional negative impacts are envisaged to occur.

On the contrary, such technical integration would avoid redundancy of data flow. Moreover, if biometric data is included in the VIS, this would lead to additional qualitative change and improvements to VISION consultation process, as it would provide authorities with means for reliable person verification. In particular the use of the fingerprint data would significantly improve the possibility to detect persons who constitute a threat to internal security. In particular these functionalities of the VIS would strengthen the horizontal task of visa authorities to contribute to the prevention of such threats for any of the Member States.

Since these background checks are carried out exclusively by the Member States, for such background checks by Member States against data in their national alert lists and data bases, the national laws implementing the data protection requirements of Directive 95/46/EC will apply.

5. Organisational arrangements for data protection supervision regime

One possible option for the data protection supervision regime could be the creation of a supervision and monitoring committee for the VIS. The legal instrument could state for example that the president of this committee is the Controller and that Regulation (EC) 45/2001 is applicable to the Committee. This would mean that there is only one legislation applicable for the VIS, with one Controller, with one supervisory authority, the EDPS, as defined in the Regulation (EC) 45/2001, and the same single legislation would be applicable to the Commission as the Processor.

[108] Article 13, Directive 95/46/EC, Article 20, Regulation 45/2001.

However, since the user of the VIS will be the Member States and their competent authorities, it seems appropriate that the personal data will be processed in the VIS on behalf of the Member States, as it is the case for EURODAC. If the Commission or other community body shall operate the VIS on behalf of the Member States, the Member States will remain controller of the data, the operator of the VIS would then act as the processor of the data [further elaborated: reference to the Eurodac Regulation, see in particular Article 3(1)]. This would imply that data controllers in the legal sense of the term, as specified in Directive 95/45/EC, would be designated authorities in the Member States. The national supervisory authorities will be responsible for the monitoring the lawfulness of the processing of data in accordance with national data protection legislation by the Member States including the transmission to and from the Visa Information System. A Community institution or a body responsible for the operational management of the system could be then designated as a data processor.

If such a model is followed, the national law of each member state transposing the Directive 95/46/EC is applicable. Each of the data controllers in Member States would have his supervisory authority as defined in the national law. The national supervisory authorities could be responsible for the monitoring of the lawfulness of data processing in accordance with national data protection legislation. On the European level, a joint supervisory authority could be established for the VIS, as it is the case for Eurodac. However, at that time the European Data Protection Supervisor has not yet been established. For this case, Art. 20(11) of the Eurodac Regulation explicitly foresees the replacement of the joint supervisory authority.

The European Data Protection Supervisor has been appointed in application of Regulation 45/2001 (which has been adopted on the basis of Article 286(2) of the EC Treaty) that require the establishment of an independent supervisory body responsible for monitoring the application of data protection acts to Community institutions and bodies.

One of the building blocks in the EC data legislation is the provision for independent supervision of compliance to the rules of data protection. The European Data Protection Supervisor is responsible for monitoring of processing personal data and ensuring the protection of individuals whose personal data are processed by the Community institutions and bodies.[109] The main responsibilities of the European Data Protection Supervisor are to advise Community institutions and bodies, handle complaints, conduct inquiries, generally observe the new developments as far as they have impact on personal data protection, intervene to grant exceptions, safeguards, authorisation and conditions for processing of personal data, register processing operations, conduct prior checks of processing operations, control data transfers, and refer the matters to the Court of Justice.

The European Data Protection Supervisor also has powers to warn or admonish the data controller, order the rectification, blocking, erasure or destruction of data when processing of data breached the data protection regulations, and impose a temporary or definitive ban on processing.[110] If the Data Controller is inside a Community

[109] Article 41, Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[110] Article 47, Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

institution or body, the EDPS has no powers to warn or admonish directly Controllers in Member States acting under national data protection law transposing the Directive 95/46/EC providing for a national supervisory control authority. The EDPS can only have warned or admonished Controllers in Member States through the national supervisory control authorities (Article 46(f)(i)).

Currently there are several channels for the co-operation between the European Data Protection Supervisor and the national supervisory authorities. The Supervisor co-operates with the national supervisory authorities to the extent necessary for the performance of their respective duties, exchanging useful information, requesting such authority or body to exercise its powers or responding to a request from such an authority or body. The European Data Protection Supervisor also participates in the activities of the Working Party on the on the protection of individuals as set up by Article 29 of Directive 95/46/EC called the Article 29 Data Protection Working Party, which allows for enhanced, institutionalised and regular co-operation in this field.

For these reasons the European Data Protection Supervisor (EDPS) should be responsible for monitoring the lawfulness of the activities of the Community institution or body responsible for the operational management of the system in relation to the protection of data.

ANNEX 4: VISA STATISTICS

Visa statistics 2001

Country	Visas Applied for	Visas refused	Visas Issued	A	B	C	D	LTV's
Belgium	170,533	11,023	150,948				19305	2428
Denmark	94,868	10,724	84,144					
Germany		482,927		25977	50662	2182158	399975	17525
Greece			481,464					
Spain			674,663	399	22910	528569	111613	7690
France	2,739,347	770,000	1,969,347	9998	64172	1757448	130615	7114
Italy			947,322					37579
Luxembourg	19,789	983	18,005					
Netherlands	399,706	33,605	326,626	26655	23710	299701	42910	15646
Austria			448,184	1293	107399	327324	12168	3946
Portugal				181	3876	121106	12462	521
Finland			407,381	14	12224	394974		169
Sweden	160,710	18,870		88	1171	129726		
United Kingdom	1,758,829	127,536	1,558,425					
Norway			85,000					
EU (including Norway and Iceland)								

Source: Guidelines for the introduction of a common system for an exchange of visa data, Council of the European Union, Brussels, 5 June 2002, 9615/02.

ANNEX 5: RESULTS OF STAKEHOLDER CONSULTATION

Introduction

This section of the report presents the results of stakeholder consultations carried out in the course of this study. These consultations have mainly focussed on the VIS with biometrics proposal (i.e. policy option 4 as described above). Nevertheless the results have been used to inform the assessment of the other options in the next section. The following consultations are reviewed:

- Commission services
- Member States replies to the Commission's questionnaire
- Public consultation
- Interviews done specifically for the study.

Each is reviewed in turn below in terms of comments on perceived costs and benefits of the VIS proposals.

Commission services

Comments and inputs from the Commission Inter-Service Steering Group, comprising representatives of various Directorate Generals and other services, have been received in connection to the interim report of the study and have been taken into account preparing this draft final report of the study.

Specific separate contributions have been received in the course of this study from the several Commission services in response to the questionnaire distributed by the DG JHA, including an interview with the data protection officer.

Member States replies to the Commission's questionnaire

Replies to the questionnaire distributed by DG JHA in connection with the EIA from the following Member States have been reviewed:

- Denmark
- Italy
- Netherlands
- Spain
- France
- Sweden
- Finland
- UK
- Estonia

- Greece
- Germany
- Hungary.

The following broad observations could be made after analysis of comprehensive replies by relevant authorities in the Member States:

- The majority of Member States remarked that there are substantial problems with the consular co-operation as exchange is based on meetings, phone calls or paper documents. Visa shopping occurs because repeat applicants present new or recently issued passports or rejection stamps are skilfully removed. Border checks are limited to the visual inspection of applicants and travel documents. Most Member States have the problem of illegal migrants arriving without documents.
- Member States did not see any alternative to the VIS as a common system for the exchange of visa data to ensure the same effectiveness and quality of exchange of information.
- The main impacts expected are in the process of visa issuing (easier assessment of application), prevention of visa shopping, and reduction in document fraud. With biometric data changing identities or manipulating documents will become more difficult. VIS with biometrics would also aid the identification of undocumented illegal migrants and speed up the return procedures.
- Most Member States view biometric functionalities as essential for the effectiveness and value added of the VIS.
- Border checks might be slower, but some Member States expect quicker processing procedures for frequent travellers, VIPs, and low risk groups.
- Opinions are divided over the usefulness of integrating scanned documents. Some Member States are sceptic about the use of scanned documents and fear large costs, other Member States are in favour to integrate scanned documents.
- In terms of processes and organisational issues, most Member States will have to adapt their national systems to the VIS, and consular posts will be most affected by such change. Changes in national legislation are also anticipated by some Member States.

Public consultation

The following contributions submitted in the process of public online consultation on the VIS have been examined:

- Immigration Law Practitioners' Association (ILPA)
- Standing Committee of experts on international immigration, refugee and criminal law
- State Data Protection Inspectorate of the Republic of Lithuania
- Contributions from private persons.

The following observations could be made from the analysis of these responses:

- Most consultees expressed a view that VIS is a disproportionate response to the perceived threats posed by third country nationals travelling to the EU. Most travellers are lawful travellers since visas issued significantly outnumber visas refused and since most of them comply with immigration requirements. The SIS, if operated efficiently, should be sufficient to counteract the security threats posed since it records information on persons suspected of criminal activities and for whom negative immigration decisions have been taken.
- There is a concern that a system like VIS is contemplated before any attempts are made to reform and improve the current system for issuing Schengen visas. In this context, a recommendation was made to amend the ambiguous rules of Common Consular Instructions which provide for a large degree of discretion in making visa issuing decisions.
- VIS so far has been presented in the repressive terms, i.e. as intended to catch criminals and abusers of the visa system. There has been no examination to what extent VIS would have positive effects for regular travellers to the EU.
- Data protection and privacy concerns have loomed large in the public consultation. In particular, concerns over the inappropriate use of data and unauthorised access have surfaced. There is also a fear that the rejection of previous visa application would automatically result in a future rejection. In addition, a recommendation was made that VIS includes only 'hard' data and not improvable facts or suspicions by authorities. Security of processing of personal data must also be ensured to prevent any possibility of identity fraud, hacking or abuse from the unauthorised access.
- Legal safeguards and rights of third country nationals should be included in the VIS and third country nationals must be made aware of these rights.
- There is also concern over the storage of personal data of EU citizens issuing invitations to third country nationals as it would constitute an invasion of their privacy.

A separate consultation was undertaken with the representatives of the travel industry, the European Travel Commission (ETC), a representative body of 33 national tourism organisations, charged with promoting tourism to the EU. The following main points were discussed in the consultation.

- The main benefit from the establishment of VIS would be for repeat visitors in terms of simplification of repeat visa applications, which is a welcome development. From this point of view, collection and sharing of visa data should be welcomed as facilitation of visa application, as long as data protection is fully enforced.
- Any form of VIS should bring more transparency to the visa application process and make it more accessible and easier for visa travellers. Europe must be perceived as a place of welcome, and VIS should not be about policing the issuance of visas, but facilitating the application process and providing ease of access for business and leisure travellers. It would be even better if VIS could lead to reduced queues and improve some of the treatment of visa travellers. If consular authorities have access to the right information about the person, especially in the repeat application, that could make the service more professional, more successful and speedier.

- The policy of transparency and ease for genuine visitors should be explicitly promoted to visa applicants. The publicity campaign should be sensitive and take into account the cultural and social circumstances in different countries. The publicity campaign should also emphasise that VIS would make people safer by giving better control over who is entering the EU, and ensuring no terrorists slip through.
- It can be expected that most genuine visitors will have nothing to hide and will provide biometric data. They would accept a trade-off between providing personal information and safer and easier travel into Europe. This would be especially so if providing biometric data will mean that subsequent issuing of visa is a 'stamp of approval' and will guarantee entry into the EU.
- Small number of people will find the taking of biometric data intrusive and unacceptable and may refrain from travelling into Europe. Therefore, authorities should research particular markets, and cultural-religious sensitivities to biometric data.
- It can be anticipated that in the short term VIS would cause negative impact, and authorities need to be prepared for that through a PR campaign. It should be focused on end-customer, and explain why, for whom, and what benefits the system will bring to the traveller.
- The negative impact could occur if access to information is wide. There needs to be restricted access to personal information to the 'right' people. Perhaps the idea of levels of access could be implemented, whereby only in the highest level of access authorities would have access to the full file. The problem of identity theft cannot be ignored, and personal data on VIS would be attractive to hackers.

The consultee also stressed the following:

- Access to the data should be controlled;
- The data held should be limited to what is necessary for the examination of visa application;
- The possibility of electronic (online) application should be investigated as it would benefit the bona fide third country travellers.

ANNEX 6: SOURCES OF INFORMATION

A number of information sources have been used in the course of this Extended Impact Assessment.

1. The Study has reviewed replies received from 12 Member States distributed by DG JHA in connection with the study for the EIA. Responses from the following Member States have been reviewed:
   - Denmark
   - Italy
   - Netherlands
   - Spain
   - France
   - Sweden
   - Finland
   - UK
   - Estonia
   - Greece
   - Germany
   - Hungary.
2. Comments and inputs from the Commission Inter-Service Steering Group, comprising representatives of various Directorate Generals and other services.
3. Specific contributions by the following Commission services:
   - DG Justice and Home Affairs
   - Secretariat General
   - DG Internal Market
   - DG Economic and Financial Affairs
   - DG Employment and social affairs
   - DG Energy and Transport
   - DG External Affairs
   - DG Information and Society
   - DG Research
4. Contributions submitted in the process of public online consultation on the VIS. In particular:

- Immigration Law Practitioners' Association (ILPA)
- Standing Committee of experts on international immigration, refugee and criminal law
- State Data Protection Inspectorate of the Republic of Lithuania
- Contributions from private persons.

5. A meeting was held to discuss specific data protection issues with the Commission's Data Protection Office.

6. A meeting with representative of the European Travel Commission.

7. Results of workshop with the experts from the Member States organised on the 27th September 2004.

8. Documents, reports and studies available in the public domain have been reviewed in the desk research phase.

A Common Policy on Illegal immigration, 37th report from the Select Committee on the European Union, House of Lords, UK, 5 November 2002.

Annual Report on Asylum and Migration 2001,. European Commission.

'America's Digital Welcome Mat', by Cynthia L. Webb, http://www.washingtonpost.com

Biometrics Deployment of Machine Readable Travel Documents, ICAO assessment report, 19 May 2003.

'Biometrics proposals raise more questions than answers', A Press Release by European Liberal Democrats, 2 March 2004.

'Biometric cards will not stop identity fraud' 21 November 2003, New Scientist. http://www.newscientist.com/news.

'Body Check: Biometrics Defeated', by Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, 3 June 2002, http://www.extremetech.com.

Cholewinski, Ryszard, Borders and Discrimination in the European Union, Immigration Law Practitioners' Association London, Migration Policy Group Brussels, 2002.

Common Consular Instructions on visas for the diplomatic missions and consular posts, Volume 46, C 310, 19 December 2003.

Communication from the Commission on Impact Assessment, COM(2002) 276 final, 5 June 2002.

Communication From The Commission On The Development Of A Common Policy On Illegal Immigration, Smuggling And Trafficking Of Human Beings, External Borders And The Return Of Illegal Residents. Brussels, 3.6.2003, COM(2003) 323 final.

Council Conclusions on the introduction of Visa Information System, 6535/04, 19 February 2004.

Council Decision establishing the Visa Information System (VIS) (2004/512/EC), 8 June 2004, OJ L 213/5.

Development of the Schengen Information System II and possible synergies with a future Visa Information System, COM (2003) 771 final, 11 December 2003.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

European Parliament report on the Commission proposal for a Council decision establishing the Visa Information System (VIS), 7 April 2004, A5-0262/2004, 7 April 2004.

European Business, Facts and Figures, Panorama of the European Union 2003, Office of Official Publications of European Communities, Luxembourg, 2003.

Fingerprint Vendor Technology Evaluation 2003: Summary of results and analysis report, NISTIR 7123, June 2004

First annual report on the activities of the EURODAC central unit, Commission staff working paper, SEC (2004).

First report on the implementation of the Data Protection Directive (95/46/Ec), COM(2003) 265 final, 15 May 2003.

Guidelines for the introduction of a common system for an exchange of visa data, 9615/02, 5 June 2002, Brussels.

Identity Fraud: a Study, UK Cabinet Office, 2002.

Maintaining security within borders: towards a permanent state of emergency in the EU? Joanna Apap and Sergio Carrera, Centre for European Policy Studies Brief No 41, November 2003.

9/11 Commission Report, http://www.9-11commission.gov/report/index.htm.

Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking into account of the establishment of the European information system on visas (VIS), 11 August 2004, Article 29 Data Protection Working Party.

Organised illegal immigration into the European Union, Europol report, January 2004.

'Privacy best practices in Deployment of Biometric Systems', 28 August 2003, BIOVISION report by Astrid Albrecht.

Proposal for a Council decision establishing the Visa Information System, COM(2004) 99 final, 12 February 2004.

Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas and a Proposal for a Council Regulation amending Regulation

(EC) 1030/2002 laying down a uniform format for residence permits for third country nationals, COM(2003)558 final, 24 September 2003.

Proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports, COM(2004) 116 final, 18 February 2004.

Regulation 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin convention, 11 December 2000.

Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, 18 December 2000.

Regulation 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, 29 April 2004.

Report from the European Parliament on the Commission proposal for a Council decision establishing the Visa Information System, 7 April 2004.

Security and Privacy for the Citizen in the post-September 11 Digital Age: a prospective overview, Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs, July 2003.

SIRENE manual, 2002/C 38/01.

Sixth report on the activities of the Joint Supervisory Authority of the Schengen Information System, January 2002-December 2003.

Statewatch, From the Schengen Information System to SIS II and the Visa Information System: the proposals explained, Statewatch analysis by Ben Hayes, February 2004.

Study on the deployment and interoperability of electronic and biometric authentication and identification, DG Information Society, June 2003.

Study on the links between legal and illegal migration, Communication from the Commission, COM(2004) 412 final, 4 June 2004.

Trafficking of human beings: a Europol perspective, Europol, January 2004.

'UK to roll-out biometric border control system', 15 June 2004, eGovernment news at http://europa.eu.int/ISPO/ida/jsps/index.jsp.

United States Visitor and Immigrant Status Indicator Technology, Assessment by the Electronic Privacy Information Center, http://www.epic.org/pirvacy/us-visit.

US VISIT, Congressional Research Service Report for US Congress, 18 February 2004, RL32234.

US-VISIT Program, Privacy Impact Assessment, US Department of Homeland Security, 18 December 2003.

US Visa Worries Deter Foreign Students', in The Financial Express, Vol XI, No 252, 31 July 2004.

VIS feasibility study final report, DG Justice and Home Affairs, April 2003.

Working documents on biometrics, Article 29 Data Protection Party, 1 August 2003.

World Travel Trends, 2003 – 2004, Forecast Forum: WTM Global Travel Report.

World Tourism Organisation World Tourism Barometer, Volume 2, No. 1. January 2004; The 9/11 Commission Report.