COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 28.12.2004
SEC(2004) 1628

COMMISSION STAFF WORKING DOCUMENT

Annex to the

Proposal for a Regulation to the European Parliament and to the Council

concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas

EXTENDED IMPACT ASSESSMENT

{COM(2004)835 final}

TABLE OF CONTENTS

1. PURPOSE OF THE EXTENDED IMPACT ASSESSMENT

The establishment of the Visa Information System (VIS) represents one of the key initiatives within the EU policies aimed at supporting stability and security. Given the potential for significant impact arising from action in this field, the Commission, in its Annual Policy Strategy for 2004, decided that an Extended Impact Assessment should be carried out. The Commission further decided that the responsible services (Directorate General Justice and Home Affairs) due to the significant crosscutting impacts and the high political significance would be assisted by an inter-service steering group including the most concerned services. This decision ensured that horizontal multi-sectoral aspects, in particular economical and social impacts could be taken into account in the process as early as possible. The task of this steering group was to define the scope, to monitor the progress of the Extended Impact Assessment and to supervise the completion of the impact assessment report.

The Commission decided further to consult an external contractor, who had to provide the Commission with a wide range of supporting services to assist the responsible services and the inter service steering group in the preparation and conduction of the Extended Impact Assessment. These services consisted of analysis of existing data, collection of additional information and providing general advice or studying specific points (e.g. data protection and the use of biometrics).

The Contractor provided the methodological tools in line with the Commission's guidelines and the handbook on impact assessments. He carried out an integrated assessment of the direct and indirect impacts of a range of policy options, defined after careful analysis of the problems and objectives by using the appropriate analytical methods and participatory approaches in the framework of the meetings of the Interservice Steering Group and with Member States experts. The Extended Impact Assessment focused on the estimation of the potential impacts of various options under consideration for the VIS. Economic/financial impacts were taken into account as well as social/political ones. Furthermore proportionality of the storage and the use of data as well as data protection issues have been considered.

2. PROBLEMS IN THE CURRENT SITUATION

The Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders between the Benelux countries, Germany and France aimed at the abolition of the checks at internal borders. The Schengen Convention created a common area where checks at internal borders are abolished and checks at external borders for all Schengen States were to be carried out in accordance with a common set of rules. Another flanking measure of the lifting of internal border controls is common visa policy. Currently there are 15 States which apply in full the Schengen acquis on visas. These Schengen States are 13 Member States of the European Union plus Norway and Iceland. Furthermore an Agreement between the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen acquis was signed on 26 October 2004 but needs to be ratified. Neither the United Kingdom nor the new Member States, which acceded the EU in May 2004, are currently participating in the common visa policy. At present there are 134 third countries

whose citizens are required to have a visa issued by a Member State to enter the territory of Schengen States. Current statistics show that Member States receive about 12 million visa requests per year. Based on these figures, it is expected that the number of visa requests will reach 20 million as of 2007, taking into account the new Member States.

The study has identified the following main problems inherent in the current situation:

2.1. Inefficiencies in the implementation of the common visa policy

Currently a third country national can obtain a Schengen visa and travel freely within the territory of Schengen States. However, information about his 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(s) of his last visa application(s) is/are not readily available to the consular authorities of the other Member State. Also, when a third country national is refused a Schengen visa, the record of the rejection is routinely stored by the authorities of the Member State which refused the application. Apart from a rejection stamp in his passport (which can easily be removed or a new passport obtained) authorities of other Member States do not know about such a refusal, when the same person applies for another Schengen visa to the authorities of another Member State.

There is some exchange of visa data in the current situation such as local consular cooperation and VISION consultation. VISION is a Schengen consultation network established for the purpose of consultation on visa applications between central authorities of the Member States. It is a message exchange system, based on the bilateral exchange of information. The study came to the conclusion that the existing information arrangements are partial, time consuming and can be inaccurate. The existing kind of exchange of information does not ensure that the information is always available in a timely fashion.

2.2. Visa application fraud and travel document fraud

There is a sizable proportion of people who currently try to obtain a Schengen visa on dubious grounds. In Germany for example, around 15% of all visa applications were rejected or visas refused in 2002. 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 new counterfeit or falsified passports without it becoming immediately apparent to consular or border check posts. Information on stolen or false travel documents and information on dubious references to support visa applications (persons or companies) is not readily available to consular posts and border checking points. The study concluded that the existing system for exchanges of information does not ensure that information reaches the missions or border control points that require it and need it on time.

Statistics from several Member States show that there is a large scale of travel document fraud. In France, 13,952 persons were carrying false documents in 2002 which was a rise of 14% compared to 2001. These fraudulent documents are either complete counterfeits or documents genuinely issued to another person having been altered without authority. Often such original documents have been stolen from or

lost by the genuine holder. Skilled forgers produce extremely convincing copies of passports and other identity documents, and of other documents needed to obtain them such as birth certificates.

2.3. Visa shopping

There exist multiple forms of bypassing the criteria for the determination of the Member State which is responsible for the examination of the visa application (known as "visa shopping"). In particular, after refusal of a Schengen visa by one Member State, the same applicant 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.

2.4. Limitations of checks at external borders

Existing border checks are based on the examination of the holder of the document, of the document itself, and of any visa contained. In making such checks, border control officers rely on the passports shown to them. 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 is a time consuming procedure. One difficulty experienced by those control authorities seeking to exchange information is that their counterparts in other countries may be part of different authorities. The same applies for checks within the territories of Member States.

2.5. Illegal Immigration

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 have been removed and around 1.2 million non EU-citizens have been refused entry.

The study showed that illegal immigration may result in a number of different modus operandi:

- By entering clandestinely
- By using counterfeit or falsified travel documents or visa
- By using false or falsified supporting documents (e.g. regarding the financial background) or making false or falsified statements in order to obtain a visa
- By "visa shopping"
- By overstaying. Where statistics exist, they show that the overstayers are the biggest number of illegal immigrants.

Many of the apprehended illegal immigrants have no travel or other identification documents with them or use counterfeit or falsified documentation. In such cases the

identification process is slow, time consuming and expensive. In case people have destroyed their travel documents, authorities currently do not have a readily available system to check the identities of the undocumented illegal immigrants.

2.6. Application of the Dublin II Regulation

The "Dublin II" Regulation (EC) No 343/2003 defines the criteria for determining the State responsible for examining applications for asylum. A basic criterion for that responsibility is whether a Member State has issued to the asylum seeker or extended a visa. At the moment, 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 an asylum application. Moreover such information would also be needed for examining the application for asylum.

2.7. Internal Security and terrorism

The inefficiencies in combating visa shopping, fraud and in conducting checks are causing also inefficiencies in relation to internal security of the Member States. Criminals and suspected persons could get a visa or have chances to use a falsified visa when entering the Schengen area. Persons involved in terrorism or in organised crime usually don't travel under their own identity but alter their personal details to make identification more difficult. They are aware of the reliance placed by control authorities on intelligence and other information about those involved in terrorist activity. They may also have substantial financial backing to allow skilful, unauthorised alternations to be made to their travel documents or to obtain high quality counterfeits.

2.8. Impacts on bona fide travellers

Of all travellers applying for a Schengen visa, 20% are estimated to be regular travellers, i.e. applying for a visa several times. For these 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 with the visa and immigration requirements in the past, for example for professional drivers in the land transport sector. In cases of lost or stolen travel documents bona fide travellers have to go through a complicated process to establish their identities to acquire new travel documents. There is also a high risk 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.

3. POLITICAL OBJECTIVES AND ORIENTATION SET OUT BY THE COUNCIL

To meet the problems inherent in the current situation, the European Council decided to develop and establish a system for the exchange of visa data. The JHA Council adopted on 19 February 2004 conclusions to give the necessary political orientation on the basic elements of the VIS. According to these conclusions the Visa Information System (VIS) is "a system for the exchange of visa data between Member States, which must meet the following objectives:

(a) constitute an instrument to facilitate the fight against fraud, by improving exchanges of information between Member States (at consular posts and at border crossing points) on visa applications and responses thereto;

(b) contribute to the improvement of consular cooperation and to the exchange of information between central consular authorities;

(c) 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;

(d) contribute to the prevention of "visa shopping",

(e) facilitate application of Council Regulation (EC) 343/2003 determining the State responsible for examining applications for asylum;

(f) assist in the identification and documentation of undocumented illegals and simplify the administrative procedures for returning citizens of third countries;

(g) 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 2 of this document. 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. It should be stressed however, that it is a component of these policies and does not itself introduce new policies.

4. POLICY OPTIONS

On the basis of the problem analysis and the objectives set out above, the Commission defined four policy options which were assessed by the contractor in the study.

4.1. Option 1: No VIS

The first option highlights the situation where the VIS would not be created. However the following developments in the current situation which have potential to contribute towards the political objectives should be noted:

- Implementation of common EU visa policy, including such recent developments as making visas more secure and difficult to counterfeit, exchanges of information on visa issuing trends at local consular level and establishment of liaison officers at immigration hot spots will be further developed.

- Continuing use of VISION which is a network to support current consultation of central authorities. However, it is 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 in these specific cases.

- Current developments of SIS II result from the necessity to connect new Member States, benefit from the latest developments in the field of information technology and allow for easy introduction of new functionalities in the system. In addition, it has recently been agreed that authorities responsible for issuing visas will have access to search SIS data on blank official documents and identity papaers which have been lost, stolen or misappropriated.

- 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 persons who have lodged an asylum application. 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.

4.2. 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. 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 and are stored in a central data base. 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. This information is also stored in the central data base. People who overstay their visas would also be identified in this part of the 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.

4.3. Option 3: Visa Information System without biometrics

Visa Information System without biometrics would be an electronic system containing information about the visa applicant from the visa application form and the decisions hereto as well as the photograph of the applicant, as introduced as a security feature in the uniform sticker for the Schengen visas. 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 other competent authorities of each Member State would have access in accordance with the purposes of the VIS.

4.4. Option 4: Visa Information System with biometrics

Visa Information System with biometrics would contain all the information envisaged in VIS without biometrics (and the same access and consultation

procedures), but crucially it will also include biometric information of visa applicants such as fingerprints.

The choice of the biometric identifier should follow a coherent approach for documents and databases, as requested by the European Council of Thessaloniki. According to the VIS feasibility study, which has been submitted by the Commission in May 2003, fingerprint technology provides the required accuracy to identify individuals. Even if the biometric technology changes, fingerprint databases will still be used for a long time. Background checks to prevent threats to internal security can be done with fingerprints, contrary to for example iris technology. Further development at a later stage might enable the use of photographs for facial recognition. The current proposals for the introduction of fingerprints in the visa sticker foresee a two-finger image (flat prints). The VIS-feasibility study recommends taking a ten-finger (flat) image from the applicant. "Flat fingers" are easier and faster to take and no physical contact is necessary between the applicant and the official. However, the standards and procedures for taking the biometric data, including the obligation and specifying the exceptions for recording biometrics, should be laid down in a further legal instrument amending the Common Consular Instructions.

5. IMPACTS OF THE POLICY OPTIONS

The study assessed the relative financial, opportunity and possible retaliation costs and possible reductions in business travel and tourism as well as the impact on privacy and human rights. Moreover the benefits of the different policy options were assessed. In this context "financial costs" mean the over and above costs already incurred or anticipated under current arrangements or planned developments. "Opportunity costs" are those for visa applicants, both financial and other costs, in terms of travel time and travel costs, to apply for and obtain a visa to enter the territory of the Schengen states. "Retaliation costs" are those which would occur if the introduction of the policy options should lead to third countries imposing restrictions or additional requirements and costs on EU travellers wishing to visit the countries in question.

The impacts have graphically been indicated with symbols:

√*	impact conditional on the effectiveness of current developments and developments planned
√	Small impact
√√	Medium impact
√√√	Very significant impact
√√√√	Exorbitant impact

5.1. Benefits and costs of Option 1: No VIS

- Financial cost**:** no change

- Opportunity costs: no change

- Retaliation cost: no change

- Reductions in business travel and tourism: no change

- Impact on fundamental rights, in particular the protection of personal data and privacy: no change

There would be no additional costs or social impacts, as the current situation in visa application process remain unchanged.

- Efficiencies in the implementation of Common Visa Policy: no change

The 'No VIS' option would not improve the current lack of information exchange about visa applications. In case a visa information exchange system is not introduced, the current situation will continue, meaning that information about visa applications 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.

- Reductions in fraud and visa shopping: √*

Some document fraud reductions are anticipated through new functions of the Schengen Information System and improved security of visas. However, these developments to increase visa security are counteracted by increasing sophistication of forgery and counterfeiting techniques. 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.

- Increased efficiency of border checks: √*

Some improvements in efficiency of border checks are anticipated with the probable introduction of new functions in the SIS II (and especially biometric data). SIS II will allow for the integration of the new Member States and update the technology used in the system.

- Reductions in illegal immigration and facilitation of the Dublin Regulation: √*

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 visa policy is concerned) have already been implemented.

No improvement of the current situation due to the lack of exchange of visa data to facilitate the determination of the Member State responsible for examining the asylum application and for the examination of the asylum application.

- Contributions toward internal security: √*

Existing instruments and processes (e.g. national security agencies, Europol, Interpol) can be expected to continue to improve internal security and reduce terrorism.

- Increase efficiencies for bona fide travellers: no change

- Other spin offs: no change

5.2. Benefits and costs of Option 2: Entry-exit system.

- Financial cost: √√√√

Financial costs for an entry exit system are extremely high. 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, entry and exit posts. It can be anticipated that similar costs would apply to EU entry-exit system.

- Opportunity costs: √√

Opportunity costs for visa applicants can be expected, as applicants would have to travel to consular posts to provide biometric data. Also time will be lost at entry and exit points by providing and checking biometric data. The study comes to the conclusion that opportunity costs in this option are higher as the opportunity costs in VIS with biometrics. These costs would include the time and travel costs to travellers of providing biometric data at visa application stage and at entry and exit points. The Commission does not share this opinion as there were no additional travels to make. Checks in the VIS with biometrics could equally lead to further questioning of travellers.

- Retaliation cost: √

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

- Impact on fundamental rights, in particular the protection of personal data and privacy: √√√√

Impact of entry-exit system on human rights would be extensive, and there would be a substantial need to meet personal data protection and data security requirements in particular in view of the use of biometrics, since there would be a risk of misuse. The study comes to the conclusion that there are very significant impacts on fundamental rights. However the Commission is of the opinion that the impacts would be even exorbitant as the entry-exit-system does not only store data from the applications including biometrics but also data from the movement across the borders.

- Reductions in business travel and tourism: √

Due to the opportunity costs for visa applicants and the extensive impact of entry-exit system on privacy and human rights some reductions in business travel and tourism can be anticipated.

- Efficiencies in the 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 other objectives set by the Council for a VIS.

- Reductions in fraud and visa shopping: √√√

Considerable reductions in visa fraud (and some reduction in other document fraud) can be anticipated. The introduction of biometric data would provide a reliable base to establish the identity of visa applicants. It would help to establish a link between visa holder and traveller, and reduce the possibility of impostors travelling with visas issued to other people. Considerable reductions in visa shopping could also be anticipated. Records of previous visa applications would be readily available to consular authorities when a person applies for a visa subsequently. The inclusion of biometric data would provide a reliable basis to confirm the identity of visa applicants, 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 will be possible. 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.

- Reductions in illegal immigration and facilitation of Dublin Regulation: √√√

Efficient immigration checks could be anticipated to 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 case they have applied for a visa in the past. The absence of an exit check would reveal applicants who didn’t return after expiry of the visa.

Exchange of visa data would facilitate the determination of the Member State responsible for examining the asylum application as well as the examination of the asylum application.

- Contributions towards internal security: √√

Biometric information would allow the identification and tracking down 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 other instruments.

- Increase efficiencies for bona fide travellers: √√√

There would be substantial advantages for bona fide travellers requiring visas as past visa history could be established in the same way as VIS with biometrics. This would be especially beneficial for regular travellers, who make repetitive applications for Schengen visas. In such cases, the entry-exit-system 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. An additional advantage of an entry-exit-system/VIS with biometrics against VIS without biometrics is that biometric information would enable the identification of bona fide travellers almost beyond any doubt (e.g. in case of lost or stolen travel documents), and thus reducing the possibility of fraud and abuse of the visa system.

- Other spin offs: √√√

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 of the territory of Member States.

5.3. Benefits and costs of Option 3: VIS without biometrics

- Financial cost: √

The study showed that this policy option would carry medium financial costs. To the Community budget, the cost is estimated to be €30 million in 2004-2006 (one-off investment), and afterwards €8 million a year for running the system. These costs would cover the operation of the 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 posts of EU Member States worldwide, such costs would be €14 million one-off investment costs and €7 million annual operational costs.

- Opportunity costs: no change

No additional opportunity costs for visa applicants are expected, as there would be no change from current visa application process. The personal information of visa applicants would be collected, processed and stored in the same way as in the present situation.

- Retaliation cost: no change

- Reductions in business travel and tourism: no change

No retaliation nor reductions in business and leisure travel is anticipated, as there would be no change from current visa application process.

- Impact on fundamental rights, in particular the protection of personal data and privacy: √√

The study expects only limited impacts on the protection of personal data, since there will be no biometric data included. However the storage of data in a central European database and the exchange of data between Member States would significantly increase the number of authorities having access and potential further processing of data.

- Efficiencies in the 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. This information should not only comprise data on the visa application but also on the decisions taken thereto including the data of the visa sticker. It would ensure that records about visa applications, which are 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.

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. However, such technical integration would avoid redundancy of data flow.

- Reductions in fraud and visa shopping: √√

Furthermore some reductions in visa application fraud and visa shopping can 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. When a third country national bypasses the criteria for the determination of the Member State responsible for examining the visa application 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. The inclusion of data on persons or companies issuing an invitation or being liable to pay the costs for living during the stay would help to identify those persons and companies which issue fraudulent invitations. This would be important information in the fight against visa fraud, illegal immigration, human trafficking and the related criminal organisations which often operate on an international scale. The identification of fraudulent sponsors is not only an issue for the Member State in which the sponsor is resident. Given the international nature of illegal immigration, it seems necessary to store such kind of data at central level, in particular in such cases in which an individual, a company or another organisation has been involved in fraudulent cases dealt with by more than one participating state.

- Increased efficiency of border checks: √√

Some increased efficiency 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, the passport itself and a visa contained in it. The inclusion of visa sticker data would significantly improve checks at external borders and within the territory of a Member State, in both directions: to detect falsified visas but also to facilitate the verification of bona fide travellers.

- Contributions to the fight against illegal immigration and the facilitation of the Dublin Regulation: √

VIS without biometrics would have a minor impact in reducing illegal migration as it would remain difficult to identify undocumented illegals as such illegal migrants are unlikely to give their true identity.

Exchange of visa data would facilitate the determination of the Member State responsible for examining the asylum application as well as the examination of the asylum application.

- Contributions toward internal security: √

VIS without biometrics would have a minor impact in improving internal security and for the fight against terrorism. 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.

- Increase 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 more appropriate decisions about repeat visa applications and thus result in simplifications and shorter waiting times for regular travellers or in the issuing of multiple entry visas valid for a longer period of time.

- Other spin offs: √

VIS without biometrics will have some spin offs, also because national visa systems need to be adapted.

5.4. Benefits and costs of Option 4 VIS with biometrics

- Financial cost: √√√

The study expects very significant financial costs of this option. For the Community budget the biometrics would cost €93 million in 2007-2011 for investment costs, and afterwards €14-16 million a year for operational costs. Concerning the costs 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 (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. For 27 participating Member States, such costs would amount to around €200 million one-off investment cost and around €50 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. The total costs, mentioned below do not include the costs for the border crossing points as these costs cannot be estimated at the present time.

	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

- Opportunity costs: √√

Opportunity costs for visa applicants can be expected, as applicants would have to travel to consular posts to provide biometric data. Also time will be lost at entry and exit points by providing and checking biometric data.

- Retaliation cost: √

Retaliation to VIS with biometrics by third countries currently requiring visas for visitors from the EU should be considered as a potential risk.

- 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. 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 to Europe, especially if providing biometric data will mean that subsequent issuing of visa will guarantee entry into the European

Union as the security is higher and the identity of the travellers could be confirmed more quickly. Only a small number of people will find the taking of biometric data intrusive and unacceptable and may refrain from travelling to Europe.

- Impact on fundamental rights, in particular the protection of personal data and privacy: √√√

The collection, storage and use of highly personalised data in a EU-wide central data base, 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. The principles of proportionate and fair use of personal data and high security in the system would have to be implemented in full.

- Efficiencies in the implementation of Common Visa Policy: √√√

Further to the support of the implementation of Common Visa Policy through better exchange of information about visa applications, VIS with biometrics would ensure exact identification and verification of visa applicants. 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. Given the high costs of VIS with biometrics, Member States might decide to pool resources and proceed with common visa application centres, at least in posts where this is operationally feasible.

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.

- Reductions in fraud and visa shopping: √√√

Very significant reductions in fraud and visa shopping in addition to the impacts of VIS with biometrics are anticipated as it would be possible to identify a person applying for applications in several consulates and despite attempts to conceal true identity or use another identity. With the use of biometric data, it would be possible to identify a person disregarding the spelling of the name or 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.

- Increased efficiency of border checks: √√√

Very significant increases in efficiency of border checks are 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.

- Contributions to the fight against illegal immigration and facilitation of the Dublin II Regulation: √√

VIS with biometrics will have significant impact on the fight against illegal migration. Undocumented illegal migrants who are apprehended in the territory of Member States 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.

Exchange of visa data would facilitate the determination of the Member State responsible for examining the asylum application as well as the examination of the asylum application.

- Contributions toward internal security: √√

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 checkpoints contributes 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 identifying applicants even if they use other identities to apply for subsequent visas or cross external EU borders.

- Increase 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. This would be especially beneficial for regular travellers, who make repetitive applications for Schengen visas. 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. An additional advantage of VIS with biometrics against VIS without biometrics is that biometric information would enable the identification of bona fide travellers almost beyond any doubt (e.g. in case of lost or stolen travel documents), and thus reducing the possibility of fraud and abuse of the visa system. This would particularly be useful for professional drivers in the transport sector as their good repute record is more securely protected in this system and authorities can rely on the data provided. This helps both in getting consecutive visas and passing borders.

Visa applicants who are family members of EU citizens will continue to be under obligation to travel to the consular authorities to provide their biometric data, which would entail costs, both of travel and of time spent in the consular post. However, provision of biometric data would help to verify their bona fide status once they apply for a visa the next time. The travel of such individuals would also be facilitated at crossing external border, as the availability of biometric data could speed up border checks.

- Other spin offs: √√√

A strong stimulus for the IT industry is 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. It can be anticipated that in the short term VIS would cause negative impact for the travel industry, 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.

5.5. Impact summary table

The following table will show the costs and benefits of the different policy options[1]:

1 √:Small impact-√√:Medium impact-√√√:Very significant impact-√√√√:Exorbitant impact

Costs	Financial costs	Opportunity costs for visa applicants	Retaliation costs for EU travellers	Reductions in business travel and tourism	Impact on fundamental rights, in particular the protection of personal data and privacy
No VIS	-	-	-	-	-
Entry-exit system	√√√√	√√	√	√	√√√√
VIS without biometrics	√	–	–	–	√√
VIS with biometrics	√√√	√√	√	√	√√√

Benefits[1]	Efficiencies in implementation of Common Visa Policy	Reductions in fraud and visa shopping	Increased efficiency of border checks	Reductions in illegal migration	Facilitation of the Dublin Regulation	Contribution towards internal security	Increased efficiencies for bona fide travellers	Other spin offs
No VIS	-	√*	√*	√*	-	√*	-	-
Entry-exit system	√√√	√√√	√√√	√√√	√√√	√√	√√√	√√√
VIS without biometrics	√√	√√	√√	√	-	√	√√	√
VIS with biometrics	√√√	√√√	√√√	√√	√√√	√√	√√√	√√√

1 √*:impact conditional on the effectiveness of current developments and developments planned-√:Small impact-√√:Medium impact-√√√:Very significant impact-√√√√:Exorbitant impact

Policy options	Advantages	Drawbacks
No VIS	Low financial cost	No improvements
Entry-exit system	Substantial improvements however a huge organisation step from the current situation, risky and extremely costly to implement	Exorbitant financial costs Very extensive impacts on privacy 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 substantial contribution to fight against illegal migration Considerable impacts on privacy and fundamental rights
VIS with biometrics	Substantial improvements in most domains	High financial costs and high indirect costs No data on exits Extensive impacts on privacy and fundamental rights Risk of retaliation

6. FLANKING MEASURES TO BALANCE NEGATIVE IMPACTS

Since the VIS is an instrument of the first pillar, the community legislation on data protection (Directive 95/46/EC and as far as a Community body is processing data Regulation (EC) 45/2001) is applicable. These rules ensure the protection of privacy and fundamental rights of third country nationals applying for visa as well of EU citizens issuing invitations with regard to the processing of their personal data. Since background checks against data in their national alert lists and data bases are carried out exclusively by the Member States, the national laws implementing the data protection requirements of Directive 95/46 will apply, as it is currently the case for the consultation between central national authorities.

As outlined in the study Member States shall provide inter alia that personal data must be processed fairly and lawfully, that they are collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Furthermore the processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed, it must be accurate and, where necessary, be kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified.

To balance the negative effects of the abovementioned drawbacks the following flanking measures should be considered:

6.1. Proportionality of the data stored

A basic requirement for proportionality and data protection is that the personal data collected are adequate, relevant and not excessive in relation to the purposes for which they are necessary collected. Since the VIS itself shall primarily support the implementation of the common visa policy only these data shall be stored in the VIS which are gained upon the visa application and the decisions taken thereto and which are needed for the exchange of visa data between the Member States to meet the objectives of the VIS.

The source for the alphanumeric personal data should be the visa application form. As not all data are needed after a decision has been taken, the storage of all these data in each case would be disproportional. To balance this effect, one should foresee two sets of data, one for each application and one added in case that further data are needed for the purpose of the consultation between central authorities, because only for about 20% of the visa applications such consultation between central authorities is needed. For this purpose the integration of the technical functionalities of the VISION network for this consultation, would not only avoid redundancy of the data flow but improve the current consultation and the related background checks in national databases according to the national law.

6.2. Disproportionality of the storage of scanned documents

The Council Conclusions foresee the storage of scanned documents in the VIS, as a possible further step in addition to the inclusion of alphanumeric data, the

photograph and biometrics. However, the study came to the conclusion that the storage of scanned documents could not be considered as proportional.

A major obstacle for effective return is uncertainty concerning the identity of the person concerned and/or his or her lack of necessary travel documents. Countries of origin often delay or deny the issuing of return travel documents because of missing information on nationality or identity. In order to avoid removal, illegal residents may therefore hide or destroy their travel documents and frequently claim a completely false identity and/or nationality. As a consequence, lengthy and expensive procedures have often been conducted, which include presentation of the returnee at several embassies of third countries or conducting a language or dialect analysis.

However, if all travel documents are scanned in the Consular posts and stored in the VIS, this would mean that for all visa applicants, estimated at 20 million per year, an extra operation at the Consular Posts would be needed. Eurostat figures show that annually only around 350,000 persons who are illegally present in the EU territory are apprehended; meaning that at least 98% of the scanned documents never will be used for identification of illegal immigrants. On the other hand, the alphanumeric data on the travel document should be in any case introduced in the VIS as well as the visa issuing authority

Furthermore, the travel documents are currently photocopied and stored in the consular post. If a Member State requires copies of these documents for returning an illegal immigrant, the competent authority can use the VIS to localise the consular post that stores the documents, and may even use the VIS infrastructure to ask for these documents. The travel documents can subsequently be faxed or sent by normal mail to the competent authority that needs them, in case that the alphanumeric data on the travel document which are stored in the VIS are not sufficient for the specific purpose.

6.3. Proportionality of the use of data

In accordance with data protection legislation, the access should be given to the data stored in the VIS only for specified, explicit and legitimate purposes. This means that the authorities which should have access to the VIS have to be defined by the specific purpose. Therefore the access for consulting the data should be reserved exclusively to duly authorised staff of the authorities of each Member State which are competent for the specific purposes of the VIS and limited to the extent the data are required for the performance of the tasks in accordance with these purposes. Access to enter and up-date the data should only be given to duly authorised staff of the consular post or another visa authority competent for examining the visa application. Therefore it is essential for the legal instrument, to define the purposes for which the data stored in the VIS may be used, the data which could be used for the specific purposes and the search criteria, which would allow access to these data in case of a “hit”, indicating that the data are stored in the VIS.

For the purposes of examining the application all information stored in the VIS may be relevant. Therefore the competent visa authority may have access to the complete application file and the linked application files of previous applications of the

applicant and of group members. To prevent threats to internal security, in particular fingerprint data may be used for background checks in national databases.

For checks on visas to verify the identity of the person who presents the visa with the applicant and/or to verify the visa presented or claimed to be issued, the competent authorities for carrying out checks at external borders and within the territory of the Member State, could have access to the data taken from the application form, the photographs and the data on the decisions of the visa authorities.

For the purposes of identification and return of illegal immigrants the competent immigration authority could have access to the complete application file and the linked application files of previous applications of the applicant and of group members.

For the purposes to facilitate the application of the Dublin II Regulation the competent authorities should have access to consult the relevant data of the visas issued or extended. Furthermore the Dublin Regulation provides that each Member State shall communicate to any Member State on request such data. These data on visas concerning the asylum seeker may be used for examining asylum applications as is appropriate, relevant and non-excessive. For these purposes the competent asylum authorities should have access to all alphanumeric and photo data stored in the VIS.

For the purposes of reporting and statistics, the competent visa authorities should have access only to the VIS for data which do not allow identifying individual applicants. This makes reporting and statistics possible for the Member States but does not give any possibility to conclude on the individual person behind these data.

6.4. Data protection safeguards

The very principles for a legal framework of data protection are already laid down and recognised at European level, in particular in Article 8 of the European Charter of Fundamental Rights, Article 8 of the European Convention of Human Rights as well as in the Data Protection Directive 95/46/EC and the Council of Europe Convention of 1981 for the Protection on Individuals with Regard to Automatic Processing of Personal Data. The above-mentioned principles must be read alongside Article 6 of the Treaty on the European Union which declares that respect for human rights and fundamental freedoms is one of the principles on which the Union is founded.

For the determination of the retention period it has to be taken into account that for reasons of data protection, personal data should be kept no longer than it is necessary for the purposes of the VIS. If personal data should be retained only for the period of the visa's validity, the contribution to these purposes 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 time period 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. However, for the start of the retention period it should be distinguished whether a visa has been issued, a visa has been annulled, revoked or extended or if no decision

has been taken on the application. It should be ensured that the data on the application should be automatically erased after the retention period has expired.

Furthermore in case that a third country national has required the nationality of a Member State, all data on this applicant shall be erased immediately as soon as the Member State responsible becomes aware of that fact.

Applicants, but also persons issuing invitations shall be informed according to Article 10 of Directive 95/46/EC by the Member State which enters the data in the VIS. In relation with the applicant the information that the data from the application form, the photograph and the fingerprints should be processed in the VIS and about his/her rights should be provided on the visa application form. Persons issuing invitations should be informed about the processing of their data by the related forms.

An effective data protection regime needs an independent data supervisory regime. 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. This implies that the data controllers are within the Member States. Therefore the national supervisory authorities should be responsible for the monitoring of the lawfulness of the processing of data in accordance with national data protection legislation by the Member States. This monitoring includes in particular the transmission to and from the VIS and the use of the data. For the reasons given in the study, it is appropriate that the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Commission or another operational EC body in relation to the protection of personal data.

7. MONITORING AND EVALUATION

The effective monitoring of the VIS requires evaluation in regular intervals. For these purposes it is necessary that systems are in place to monitor the functioning of the VIS against objectives, in terms of outputs, cost-effectiveness and quality of service. The study recommends that every 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.

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.

Monitoring and evaluation indicators could be in particular:

– System availability rate

– Number of entries on the system

– Numbers of visas refused, annulled, revoked indicating the standard grounds

– Number of repeat applications in the 12 month period after a visa refused.

Other indicators could be based on national statistics such as:

– Average time taken to process an application

– Processing times at border checkpoints

– Average application processing time

– Number of illegal immigrants identified

– Number of visa hits for the Dublin Regulation

8. STAKEHOLDER CONSULTATION

The Extended Impact Assessment had to ensure that the relevant stakeholders, in particular the Member States but also data protection authorities and the interested public have been involved and consulted as regards the different competences touched upon by the proposal in compliance with the Commission´s standards on consultation.

Stakeholders' consultations were held between April and July 2004. In several workshops experts from the Member States contributed with their input to the Extended Impact Assessment. Furthermore the public had the possibility to comment on the possible impacts of the establishment of the VIS. Moreover an interview with the European Travel Commission (ETC), a representative body of 33 national tourism organisations has been conducted.

8.1. Member States

The study has reviewed replies received from 12 Member States to the questionnaire distributed by Commission Services.

- 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 apprehended 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 of integrating 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.

8.2. Public consultations

The contributions submitted in the process of public online consultation on the VIS have been examined including those from Immigration Law Practitioners' Association (ILPA), Standing Committee of experts on international immigration, refugee and criminal law, Data Protection Authorities and 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 consulted in a systematic way, should be sufficient to counteract the threats posed since it records information on persons who should be refused entry to the Schengen area.

- 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 proposals so far have been presented in the repressive terms, i.e. 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 a 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.

- The main benefit from the establishment of VIS would be, according to the tourist industry, 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. 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. People should be treated in a civilised way, and not like second class citizens.

- The idea of electronic visa application should be looked into. Australia has this, and travellers can apply electronically, or via a travel agency. If biometric data is introduced, there could be places like travel agencies, or passport issuing offices, where travellers could provide their biometric data (it was not clear whether this would be possible in the VIS).

9. COMMISSION DRAFT PROPOSAL AND JUSTIFICATION

9.1. Proportionality and European added value of the options

Based on the assessment of the four options in chapter 5, proportionality and the European added value of the options can be summarized as follows:

	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	Substantial improvement, however huge organisation step from the current situation, risky and extremely costly to implement	As VIS with biometrics but also enables comprehensive immigration controls
VIS without biometrics	Improvement of the current situation but would meet only some of the political objectives	Facilitates exchange of information on visas on a regular and comprehensive basis to enable implementation of common visa policy
VIS with biometrics	Despite of extensive impacts on fundamental rights and high costs this option would tackle many of the problems identified and meet political objectives set out. By introducing the abovementioned flanking measures the extensive impact will be counterbalanced	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

9.2. Final Policy choice

The assessment of the different parameters shows that option 4, the establishment of a Visa Information System integrating biometric identifiers is the option which closely meets the objectives and purposes outlined in the Council Conclusions of 19 February 2004. In a large database it is not possible to identify persons with alphanumeric data alone. Even for bona-fide travellers the spelling of the same name can be different from one country to another, many instances of the same name exist and in some countries dates of births are not completely known. Identifying undocumented persons or persons is virtually impossible without biometrics.

Inclusion of biometric data in the VIS would not only significantly support the assessment of applicants in view of preventing 'visa shopping', fraud and threats to internal security, but have positive consequences for bona fide travellers. Matches against biometric data would help to verify their identity in case of a new application or at checks, but also in case of lost or stolen travel documents as bona fide travellers could quickly prove their identity to get new travel documents and visas. Moreover, the inclusion of biometric data would also significantly support the identification of undocumented illegal immigrants and the return procedures, if these illegal immigrants have once applied for a visa.

An EU entry-exit system, incorporating biometrics for visa applicants would provide a continuum of measures to control the movements of third country nationally, from a visa application stage through arrival at external border to leaving the territory of the Schengen states. Such a system would enable much more efficient and effective border controls to be operated. There also would be improvement to immigration control arrangements, overall, due to the existence of more comprehensive records. However it would be extremely costly to implement. It therefore appears to be less advantageous than VIS with biometrics. A VIS without biometrics would ensure improvement of consular cooperation but would have little impact as a contribution towards internal security and fight against terrorism and on the fight against illegal immigration. Furthermore bona fide travellers would profit to a small extend from a VIS without biometrics as there were just some improvements in the visa issuing process but no improvement in case of lost or stolen travel documents as they could not proof their identity quickly. Option 1 (No VIS option) would not create improvements in exchanges 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 and therefore this option would not achieve the objectives of the Council Conclusions of 19 February 2004.

For the preparation of the proposal the flanking measures outlined in section 6 of this document should be born in mind in order to minimize and balance the negative drawbacks of the chosen option.