PROJECT: **Visa Information System** CONTRACT N°: **08370500**	TRASYS
Document title: **Final Report** Document code: 08370500/TI.10.10/Final Report.doc/V2.0	

CIRCULATION / DISTRIBUTION LIST

Name	Address	I/A	Name	Address	I/A
Luc WAGNER	DG-JAI	I	Rudolf ROY	DG-JAI	I
Wilhelm HEYER	DG-JAI	I	Bert ELEVELD	DG-JAI	I/A
Peter HANEL	DG-JAI	I	Pascal MILLOT	DG-JAI	I
Erik Jan ROGGEKAMP	DG-JAI	I	Frank PAUL	DG-JAI	I/A
Jan De CEUSTER	DG-JAI	I	Sylvia KOLLIGS	DG-JAI	I
Horst HEBERLEIN	DG-JAI	I/A	Richard Ares BAUMGARTNER	DG-JAI	I

(I = for information, A = for action)

STATUS INFORMATION

Security classification:	Restricted to Members of the Project	State:	Final
Current version number:	V2.0	Date of first issue:	17/03/03
Prepared by:	Trasys Project Team	Date:	28/04/03
Verified by:	J.P. Cornet	Date:	28/04/03
Approved by:	D. Dzierzgowski	Date:	28/04/03

DOCUMENT CHANGE RECORD

Version	Date	Description	Affected sections
1.0	17/03/03	First release to DG-JAI	All
1.1	18/04/03	2nd Release to Member State review.	All
2.0	28/04/03	Release for final acceptance	All

EXECUTIVE SUMMARY

What is the background and scope of the study?

Following the European Council meeting in Laeken in December 2001, the European Commission was invited by the Council to conduct a feasibility study on a common European **Visa Information System (VIS).**

Council guidelines, adopted on 13 June 2002, define the VIS **as 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 co-operation 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 the Dublin Convention 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.

The scope of the feasibility study launched by the European Commission is to provide an analysis of the technical and financial aspects of the Visa Information System (VIS), based on the technical and functional guidelines for the feasibility study, as set out in part II of the Council guidelines. The study does not cover an assessment of the existing national systems, but considers their interoperability with the VIS system.

What are the primary processes to be supported by the VIS?

VIS will be a unique common system for the exchange of visa data between Member States**.** It should support the primary processes of visa issue and VIS consultation.

Visa issue deals with visa application registration, application assessment and issuing decision. This process integrates the functionality of the Schengen consultation network VISION as well as initiates the SIS II consultation for every new visa application in order to determine whether an alert has been issued on the applicant for the purpose of refusing entry.

VIS consultation supports the verification and identification of visa applicants. This process can also be used to assist the identification of persons in order to return aliens or to determine the State responsible for asylum applications under precondition that these persons have once applied for a visa and thus their data have been entered into the system during the visa issue procedure. The consultation also supports the authentication process of a visa sticker and the control of a visa carrier at cross-border checkpoints, as well as the verification that the carrier and the holder of a visa are the same person.

What are the basic options and solutions for the architecture?

As stated by the Council guidelines, the structure of the VIS must be similar to that of the existing Schengen Information System (SIS). The SIS system is composed of a Central System and a National System. Similarly, the future VIS system will comprise of a central visa information system (C-VIS) and, in each State, a national system with an interface to the central system (N-VIS). The consular posts and other national authorities (border checkpoints, police and immigration authorities) will need to connect to their corresponding N-VIS to benefit from the VIS services.

Therefore the Visa information system implies consideration of three levels:

- **Central level**, referred to the **Central Visa Information System** (**C-VIS**), under a single responsible authority, to be decided;
- **National level**, for each Member State, comprising national systems and their interfaces to the C-VIS (**National Visa Information System, N-VIS**);
- **Local level,** which includes the consular posts, the border crossing points, the immigration and police authorities.

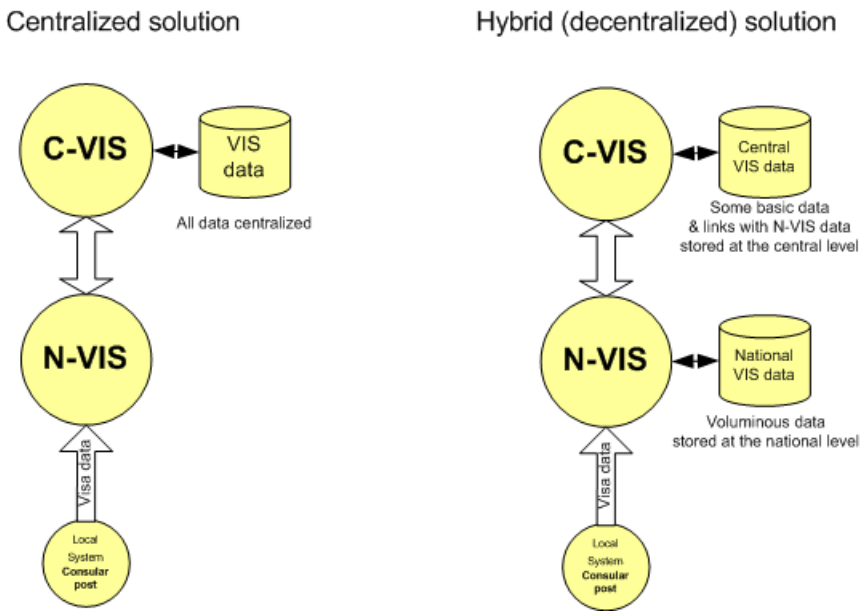
Taking into account the above context, two basic architectural options have been considered: a separate VIS (option 1), and the technical integration of VIS and SIS II in view of synergies (option 2).

Option 1: Separate VIS system

For a separate VIS, several solutions have been examined from a functional, technical and operational perspective. Only two solutions, a centralised and a hybrid one, are suitable. Both solutions support the VIS business context, meet the response time requirements and meet the business continuity requirements.

In the **centralised solution**, all the data and functions are exclusively located at the central level (C-VIS).

In the **hybrid solution** only basic data (mainly alphanumeric data) is stored at the central level (C-VIS), while bulky data (photographs, biometric images, scanned documents) are stored at the corresponding national level (N-VIS).



From a **functional and operational perspective,** the centralised solution provides one main advantage over the hybrid one. In the latter the visa history of a traveller is distributed over several national systems, making the tracking of the complete visa history of a traveller a cumbersome process, involving access to a large number of national systems (N-VIS).

From a **system management perspective** the central solution is also advantageous: the system management and maintenance procedures are easier to implement, due to the single site and data centre (as well as business continuity system).

From a **financial perspective**, the implementation of a centralised solution for the VIS is advantageous to the hybrid one. In monetary terms, the **t**otal **c**ost of **o**wnership (TCO) of the centralised solution is lower compared to the hybrid one.

The overall risk associated with the centralised solution is lower compared to the hybrid one. In particular, project management and financial risks are lower, since this solution involves having to plan, set-up and roll-out one single complex system. In the hybrid solution provisions have to be made in the planning phases for the set-up, and subsequently rolling-out, of a complex system for each Member State.

Option 2: Technical integration of the VIS and SIS II

At the functional level, VIS users consult the SIS II during the visa issue to determine whether an alert has been issued for visa applicants. Similarly SIS users (border crossing points, police and immigration authorities) connected to the SIS technical infrastructure need to check visa authenticity or traveller identity, as well as to identify undocumented travellers, thus need facilitated access to the new system.

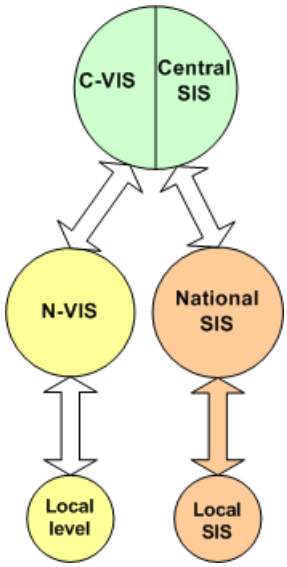
In view of the above, synergies can be envisaged between the two systems at central level, based on the assumption that SIS II would have a centralised architecture.

Feasible solutions for such synergy architecture are:

- Solution 1, **common technical platform**, deals with placing both systems in the same building, connecting them to the same network through a single access point, using the same technological platforms and share management tools and staff;

- Solution 2, **common technical platform and services**, introducing in addition to the above (solution 1) synergies at application level. Shared or common services between the systems are introduced.

Nevertheless in both these solutions, data remains separated.



Synergies will not impact the business processes. Both the SIS and the VIS users will be able to operate seamlessly in the case that the synergies are implemented. Synergies will lower the cost of ownership of the VIS and SIS II respectively.

In addition, other synergies can be achieved: VIS and SIS II could share a common business continuity system at the central level with a significant impact on costs; both projects could be developed under a common management organisation, which could oversee the project implementation starting from a common call for tender procedure for both systems.

Technical integration of VIS and SIS II at central level is recommended due to the reduction of total costs of investment and operations. In order to maximise the synergies between the systems, it is suggested to implement VIS and SIS II in parallel and even to have a common call for tender for both systems. Likewise it is advisable that the project management concerning the implementation is assumed by a single organisation.

What visa information could be stored and processed?

Data to be stored in the VIS could comprise the following categories:

- **Alphanumeric data** drawn from the uniform visa application form, the visa sticker and the data of the decision-making process (including types of visa, status, standard grounds for refusing, annulling, revoking or extending a visa and competent authority that issued the visa and whether the latter issued it on behalf of another state);
- **Digitised photograph** of the applicant;
- **Biometric information** obtained from the applicant during visa application registration procedure. Biometric acquisition is the capture of some physiological or behavioural traits of a person (fingerprints, iris, voice etc.); this will allow to uniquely identify that person or to verify an identity claimed by a person;
- **Scanned documents** supporting the visa application like travel documents or residence permits.

The VIS has been sized to support 20 million visa requests a year and a 5-year retention period. This figure has been computed by extrapolation of the current visa statistics (12 million visa requests per year) provided by the current Member States (and Iceland and Norway) and taking into account the countries in accession. It has also been assumed that 20% of visa applicants are frequent travellers and are already enrolled in the VIS database.

Having regard to the total number of visas issued yearly and considering the number of multiple-entry visas, cross-border checkpoints (entry and exit controls) would have to perform 40 million visa and traveller verifications per year. Another 5 million person identifications will be lodged in the VIS by the police and immigration authorities in charge of identifying undocumented persons.

VISION should be integrated in the VIS system. It is estimated that 20% of the visa requests will create VISION consultation, thus 4 million.

In conclusion, the VIS system should be designed to process 20 million visa requests per year, which implies sizing the system to process and store high volumes of alphanumeric data, digitised photographs, biometric data, supporting documents; such volumes can be handled by the currently available technology. Per year, it is also expected to verify on-line 40 million visas and travellers, and identify 5 million persons.

With a five-year retention period, the number of visa applications stored in the VIS would reach 100 million. However, specific information (photographs and biometrics) of applicants would only account for 70 million due to multiple applications by frequent travellers.

What biometrics identifiers could be used?

Biometric technology is capable of using traits like fingerprints, iris or face to facilitate the verification of a claimed identity of a traveller or to identify an undocumented person. The qualification of a biometric trait depends on its capability to uniquely link a biometric template

(characterised numbers extracted from the processing of a scanned image) with each individual. Such a biometric trait can be considered as an identifier of the person.

Biometrics could support the manual procedures for verifying identities currently conducted through visual checks, which are subject to human errors. It is the only means to determine if an applicant has previously applied for a visa under a different identity and to determine if the applicant has background records, when the name has changed.

Having examined several biometric identifiers only fingerprints, iris and facial could suit the VIS purpose:

- **Fingerprints** is mature technology, has shown its ability to scale to million of users. Moreover, it is the only biometric that **allows background checks against latent data stored in national systems**;

- **Iris-scan** has stability and distinctiveness as primary strengths, but it is considered as intrusive (exposure of the eye to infrared radiation). Difficulties in the enrolment process and immaturity of the technology are its major drawbacks together with the proprietary nature of its algorithm patents, which are vested to a single company. However, the market might evolve;

- **Facial** recognition can use photographs stored in the system that comply with certain high quality standards. The technology is characterised by its ease to acquire; it is non intrusive, can be used for verification only while **being far less accurate than fingerprints and iris when it comes to identification**. However the market is in its infancy. There are signs that it might attract large investment. However, the accuracy level reached so far on small trial databases should improve before the use of such a technique can be considered in the context of projects like the VIS.

Fingerprints technology provides the required accuracy to identify individuals with certainty and thus should be considered as the prime biometric solution for the VIS. Even if the biometric technology changes, fingerprint databases will still be used for the next decades.

Fingerprint technology is still becoming cheaper and the matching algorithms are being continuously improved. This would result in higher speeds and higher accuracy. This approach gives the most flexibility in terms of scaling, investment and tuning of accuracy depending on the needs and experiences. A secondary biometric identifier could be implemented (such as facial recognition) to bring back the accuracy to the appropriate level, if due to the size of the biometric database the accuracy is worsening (this could be the situation for instance in 5-7 years).

Which communication infrastructure is recommended?

- **Between C-VIS and N-VIS**

The sensitivity of the VIS information and the critical aspect of the VIS functionalities require that C-VIS and N-VISes be interconnected over a private network using strong encryption and having high availability. Each Member State should have two access points to this network (N-

VIS and its mirror N-VIS locations) with a sufficient bandwidth. Three solutions have been examined with regards to the infrastructure connecting C-VIS to the N-VISes: a **new network**, and the existing network infrastructures of **SISNET** and **TESTA.**

The existing networks, SISNET and TESTA do not meet the availability requirements for the critical process of visa and traveller verification. Neither of these networks provides the availability level of 99.9% to support this critical VIS process.

Upgrading the existing network infrastructures, SISNET or TESTA to meet the requirements is a feasible option from a technical perspective. However, in the SISNET case the current contractual arrangements expire in 2008 and cannot be extended. Similarly in the case of the TESTA II network (currently available), the contract expires in 2005.

However, according to the current IDA planning, TESTA III (the successor of TESTA II) could be seen as the new network infrastructure, which would be available in 2005.

VIS requires a completely new communication infrastructure. The set-up time for a new infrastructure would be at least 18 months and entails significant risks, administrative burden in addition to large investments.

From a strategic perspective the TESTA III should be seen as the new network. In the current state Commission Services (DG-Enterprise) have initiated a public procurement procedure for TESTA III to meet the requirements. TESTA III could be therefore the preferred communication infrastructure solution.

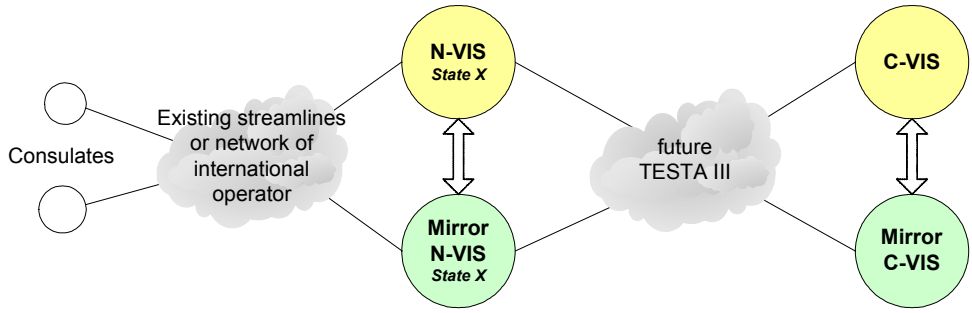
- **Between N-VIS and consulates**

Consular posts need to connect to the N-VIS via secured networks with sufficient capacity in order to have access to the VIS functionality. It is the responsibility of each Member State to establish the connectivity between their world-wide offices issuing visas and the N-VIS.

Member States with established network infrastructures connecting their world-wide visa offices to the national central authority might have to upgrade their existing communication infrastructure.

Member States, without network infrastructure connecting their consular posts, might have to start a procedure for the provisioning of such a network in anticipation of the VIS. Nevertheless, the communication requirements for connecting consular posts to the N-VIS are moderate and commonly available from international telecommunication operators today.

Member States should take appropriate measures to establish new or, if applicable, to upgrade their existing communication infrastructures between consulates and the N-VIS.



How should the VISION network be developed?

The Schengen consultation network VISION has been established for the purpose of consultation on visa applications between central authorities of the Member States. VISION is currently a message exchange system. From a business integration perspective, the VISION consultation network could be developed as part of the visa issue process. This would marginally increase the VIS application development costs. This increase in capital expenditure has been weighted against the cost savings in system and application maintenance as a result of having VISION processes integrated in the VIS application.

The VISION consultation network should be developed as part of the VIS.

Which further technical aspects have been assessed?

▪ Interoperability

The development of the VIS would be based on open and commonly adopted standards that will facilitate the integration, interoperability and data sharing with existing systems e.g. SIS II and national visa systems. Moreover, VIS should provide a programmable application interface (services) that will facilitate Member States to develop applications to make use of the VIS services.

The SIS II consultation would be executed during the visa issue procedure for every new visa application. Similarly, the SIS II users through the national interface could consult the VIS to verify visa stickers, person identities. This type of interoperability shall not by any means imply the merger of the two systems.

Interoperability should be ensured between VIS and SIS II, as well as with existing national visa systems operated by the Member States. VIS should have a component-based service architecture that could facilitate data and functionality sharing with national systems that comply to open standards and technologies.

▪ Characteristics of the technical support units

The creation of the VIS would require support at central (C-VIS) and national level (N-VIS). Support at **central level** includes the maintenance procedures and daily operation of the VIS, the training and support of Member States in using the system (help-desk). At **national level**, maintenance of the standard configurations at the consulates and other equipment, the

management of user access rights and the general co-ordination of these new supporting activities.

The human resources necessary to perform these operations could be organised in so-called Technical Support Units. These units could be created at the central (C-VIS) and national (N-VIS) system. According to the allocation of responsibilities, with regard to the new system, between the EC and the Member States, a central technical support unit (operating from the C-VIS) should be in charge of the VIS operation and the training of the Member States. Member States would be in charge of managing users (access rights management to the new system), and for training and providing a help desk to the national consular posts and authorities that make use of the VIS.

Management, maintenance and support of the VIS system should be performed by Technical Support Units acting at the central (C-VIS) and national (N-VIS) levels.

- **Technical options for the location of the C-VIS**

From a technical point of view, C-VIS can be located anywhere inside the Schengen area provided that existing communication and security infrastructures and other technical facilities are available. This equally applies to the business continuity system which should be located in a separate location.

In the case of the technical integration of the VIS and SIS II, a single location should be selected to host both the VIS and SIS II central components. The same rule applies for selecting a location for the business continuity systems.

- **Mechanisms for security measures**

Strong encryption, authentication of users, intrusion detection, monitoring and reporting should be the main security measures.

- **Technology opportunity**

The visa sticker could evolve to store alphanumeric, photograph and biometric information. The stored information could be used for off-line visa and traveller verification without connecting to the VIS. This will have a positive impact on the communication costs and availability requirements. However special equipment will be needed for this verification process.

How much time is needed for the implementation of each solution?

Two implementation scenarios have been envisaged for the rollout of the VIS, equally applicable to all the solutions. **Dates are indicative under the precondition that political, financial and legal aspects allow the launch of the call for tender procedure in 2003:**

1. **A big-bang implementation scenario** where alphanumeric data, photographs and biometrics are implemented in a single step. The supporting documents are introduced at a later stage.

Step 1 (available in 2006)	Step 2 (available in 2009)
Alphanumeric Photographs Biometrics	Supporting Documents

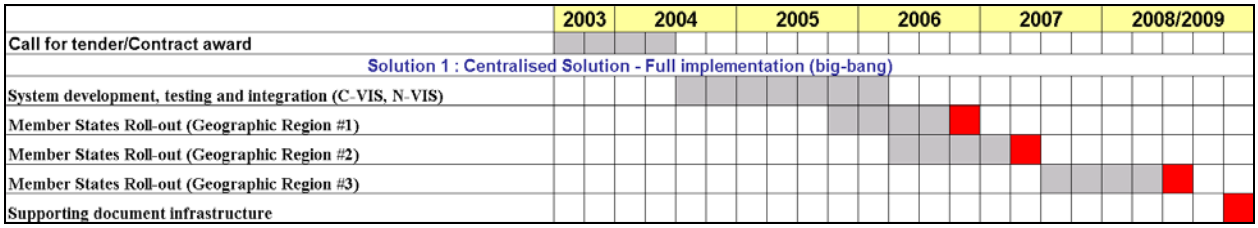
2. **A gradual (step-wise) implementation scenario** with several implementation steps starting with alphanumeric data, adding photographs at a later stage, then incorporating biometrics. The supporting documents are introduced as the last step.

Step 1 (2006)	Step 2 (2007)	Step 3 (2008)	Step 4 (2009)
Alphanumeric	Photographs	Biometrics	Supporting Documents

The implementation scenarios equally apply to the central system (C-VIS) and the national systems (N-VISes), one in each Member State.

Independently of the implementation scenarios, consular posts gradually connect to the VIS by geographic region (one geographic region after the other) as indicated in the table below. It might take about three years to provide consular post with the necessary equipment. This is the responsibility of the Member State to determine, and depends on their planning.

Below is a simplified planning for the rollout of the VIS in the **centralised solution**. A similar planning can be envisaged for the **hybrid solution**. However, it takes longer to implement due to increasing complexity at the national level (N-VIS).



Both implementation scenarios are feasible from a technical point of view. However it is recommended to endorse a big-bang implementation approach. It requires less project co-ordination, and lowers the costs for application design, testing and integration and makes the functionalities available at once at centralised level. Member States can adopt a gradual rollout planning to connect their consulates to the VIS according to national strategies and budget lines.

What is the overall impact on financial and human resources?

The study has assessed the impact on financial and human resources for four possible solutions for the architecture of the VIS, focusing on C-VIS and the N-VIS as requested by the Council guidelines. **The detailed estimates for the C-VIS and N-VIS** are provided in chapter 7 on investment and resource planning, taking into consideration the two possible scenarios of the global implementation (big-bang) and a gradual (step-wise) implementation.

The following overviews of the overall financial impacts are based on the assumptions that the categories of data (alphanumeric, photograph, biometrics, supporting documents) and the recommended biometric identifier (fingerprints) will be used for the VIS.

Total bill of expenditure for the C-VIS and N-VIS

Table 1-1: Separate VIS: Centralised architecture.

Thousands of €	Alpha	Photo	Biometrics	Documents	TOTAL
Fixed costs	10 467	2 182	144 127	1 245	**158 021**
Operational costs (annual)	6 007	8 815	24 312	1 671	**40 805**
Human resources (annual)	844	128	181	128	**1 281**

Table 1-2: Separate VIS: Hybrid architecture.

Thousands of €	Alpha	Photo	Biometrics	Documents	TOTAL
Fixed costs	39 430	14 637	142 731	721	**197 519**
Operational costs (annual)	11 467	7 746	23 045	1 297	**43 554**
Human resources (annual)	844	128	181	128	**1 281**

Table 1-3: Centralised VIS integrated with SIS II at technical level (solution 1).

Thousands of €	Alpha	Photo	Biometrics	Documents	Total
Fixed costs	10 265	1 484	143 841	1 178	**156 767**
Operational costs (annual)	5 505	4 477	22 868	1 542	**34 393**
Human resources (annual)	570	87	129	87	**873**

Table 1-4: Centralised VIS when all the synergies with SIS II are applied (solution 2).

Thousands of €	Alpha	Photo	Biometrics	Documents	Total
Fixed costs	9 033	1 359	122 287	1 030	**133 709**
Operational costs (annual)	5 277	4 456	19 622	1 517	**30 873**
Human resources (annual)	570	87	129	87	**873**

These budgets do not cover the impact on the national parts of the VIS beyond the N-VIS. For the respective assessment of each Member State the study, as indicated below, provides cost estimates for an office issuing visas on the basis of a standard configuration.

Bill of expenditure for a medium-sized visa issuing office

Table 1-5: Standard configuration for a medium-sized visa issuing office.

Thousands of €	Alpha	Photo	Biometrics	Documents	TOTAL
Investments costs (fixed)	3	1	7	3	**14**
Operational costs (annual)	2	0	2	1	**5**

CONTENTS

1. INTRODUCTION AND OBJECTIVES

1.1 BACKGROUND

Visa related fraud, visa shopping, identity theft, undocumented persons, illegal immigration, internal security and the combating of terrorism are some of the problems that Member States are confronted with.

To meet these challenges, Member States have taken important steps towards the administration of a common visa policy for the Schengen area. Member States apply a uniform visa for the Schengen area, uniform rules for the visa application and decision making procedure, consultation of national authorities and consular co-operation in the context of their common policy on the free movement of persons, with a view to preventing negative consequences as regards entry to Schengen territory and internal security.

Common policies include in particular:

- A uniform visa for the Schengen area (several types of short stay visas);
- A uniform visa application form for all travellers applying for a Schengen visa;
- A uniform format visa-sticker;
- Integration of the photograph (affixed to the uniform visa application) in the visa-sticker as the means to provide for the visual verification of the visa carrier and the holder.

The visa application and issuing procedures are determined in the Common Consular Instructions for the diplomatic missions and the consular posts. These instructions stipulate among others:

1. The types of documents aliens have to present when applying for a visa:
   - Alphanumeric data encoded manually in the uniform visa application form;
   - Photograph affixed to the uniform visa application form;
   - Supporting documents attached to the uniform visa application form.
2. The steps taken by diplomatic missions and consular posts, and by national central authorities of the Member States during the initiation of the application procedure and examination (assessment) of the visa application to decision making (e.g. visa granted or refused);
3. Instructions and models on how to fill-in the visa sticker.

In support of the common visa-issue procedures, some Member States have developed information systems that store, manage and process visa information. Information is registered by the diplomatic or consular posts and subsequently electronically transmitted to the national central authorities for examination. These systems are confined to national use and do not provide data sharing with other Member States. There is consultation of the SIS and VISION, however a**t the present time, there is no European-wide information system to facilitate the electronic exchange of visa data between the Member States and to support the administration of the common visa policy.** Recent political developments however have put

the introduction of this new system high on the political agenda of the Member States and the Institutions.

The European Council in Laeken on 14th and 15th December 2001 asked the Council and the Member States, in point 42 of its conclusions, to take steps to set up a **common visa identification system**.

Point 36 of the comprehensive plan to combat illegal immigration and trafficking of human beings in the European Union, adopted by the Council on 28th February 2002, states: *"A series of reflections and feasibility studies should be investigated and could explore whether such a common electronic system could complement the concept of security documents in order to create a dual identification process based on secure documents and a database".*

Point 37 reads as follows "*in order to ensure that the services responsible have information which is as full and helpful as possible, this database should not only contain details of visa issued but also data concerning visas applied for and refused."*

Point 38 adds that "*such a system could include information which is already gathered or required by the visa applicant today, such as personal particulars. In addition an electronic photo could be taken and stored, together with the biometric data of the applicant. Travel documents should also be scanned and stored, which would have two major advantages. First, subsequent manipulations of the travel documents could be easily detected by comparison of the travel document with its image. Secondly, the stored image of the travel documents could be used to obtain new travel documents quickly, when a person is obliged to leave the country but tries to conceal his or her identity. Anyway, the development of such a system should be based on a clear definition of needs and objectives as well as a thorough evaluation on existing initiatives (including the possibilities already offered by the SIS and VISION) and resources to be mobilised".*

1.2 OBJECTIVES OF THE VISA INFORMATION SYSTEM

According to the Council guidelines[1] for the introduction of a common system for an exchange of visa data, the new Visa Information System is a **system for the exchange of visa data between Member States.** It must meet the following objectives:

1. 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;

2. Contribute to the improvement of consular co-operation and to the exchange of information between central consular authorities;

3. 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;

4. Contribute to the prevention of "visa shopping";

5. Facilitate application of the Dublin Convention determining the state responsible for examining applications for asylum;

[1] Adopted on the 13th June 2002.

6. Assist in the identification and documentation of undocumented illegals and simplify the administrative procedures for returning citizens of third countries;

7. Contribute towards improving the administration of the common visa policy and towards internal security and to combating terrorism.

1.3 OBJECTIVES OF THE STUDY

The study aims to provide the Commission with an analysis of the **technical** and **financial** aspects of a system for the exchange of visa data between Member States, and, as requested by the Council in its Guidelines for the feasibility study, to provide a range of possible solutions that meet the objectives of the VIS, and to assess the impact of each solution in relation to these objectives.

In particular two main options have been examined:

1. A separate VIS, comprised of a Central Visa Information System (C-VIS) and one National Visa Information System (N-VIS[2]) for each Member State;

2. The possibility of a technical integration between VIS and SIS II.

As regards the first option, two solutions were examined from a functional, technical and operational point of view.

As regards the second option, the potential synergies between VIS and SIS II were examined, with a view to:

- minimising the human and financial resources required but also
- enhancing end user and functional performance.

Two solutions were also examined as regards the second option.

An additional objective of the study is to determine how to develop the VISION Network in relation to the VIS, as both systems share the same stakeholders (users). This is done through examining the means necessary to avoid redundancy of data flow via the development of VISION consultation as a part of a VIS business process.

The scope of the study does not include an assessment of the impact of the VIS on the existing systems operated by the Member States. However it considers the technical interoperability and data sharing with these existing systems. Member States will have the technical possibility to connect the existing national systems to the VIS and to benefit from the VIS functionalities and the data stored and processed by the system. The study also provides an assessment of the communication infrastructure required for an office issuing visas on the basis of a standard configuration.

[2] N-VIS should not be understood as the existing national visa systems but as a part of the new system to be set up.

1.3.1 Option 1: Separate solution for VIS

With regards to establishing a separate VIS, two solutions have been examined:

1. A *centralised* solution in which the VIS subsystems and business logic reside in one central location (C-VIS);

2. A *hybrid* solution in which the VIS subsystems and business logic are divided/distributed between the central and national systems (C-VIS/N-VIS).

For each solution:

1. *Data storage characteristics* have been examined to determine storage requirements for the various types of data (alphanumeric data, photographs, supporting documents and biometric data);

2. *Network and communication needs and constraints* have been examined to determine the communication requirements between the C-VIS and N-VIS and the communication requirements between N-VIS and consular posts;

3. *Application specifics* have been examined to determine the functions to be supported by VIS including the location from where these functions would be executed (C-VIS or N-VIS);

4. *Interoperability issues* have been examined to determine the standards needed to facilitate VIS interoperability with existing national systems as well as the SIS II;

5. *Availability considerations* have been examined to ensure VIS users never experience unacceptable service disruption;

6. *Security concerns* have been examined to determine the applicable security measures (e.g. encryption, digital signatures that could be implemented).

The impact of each solution in terms of the financial and human resources required has been detailed in an investment and resource plan. The implementation timetable and an estimated multi-annual expenditure plan (bill of expenditure) for setting up each solution has also been made available.

1.3.2 Option 2: Technical integration between VIS and SIS II

The technical integration (synergies) between VIS and SIS II has been examined with a view to maximising the sharing of human and financial resources required by the two systems. Technical integration aims to meet the challenge of interoperability and sharing of data between the systems while keeping systems logically separated, as legally required.

The synergies that have been examined are as follows:

- At a *functional* level, where integrating the functionalities of the two systems at the end-user level has been examined. In particular, VIS users as part of the routine visa issue procedure access the SIS II. Likewise SIS users capitalise on the existing SIS II infrastructure to facilitate access to the VIS functions;
- At the *organisational* level, the impact of a unified project management for VIS and SIS II through a common VIS/SIS II management centre has been examined. With regard to end-user support (help desk) and training, use of shared resources has been examined;

- At the *physical facility* level, co-housing of VIS and SIS II in one physical environment has been examined.

At the *technology* level, two alternatives were examined:

1. The development of a *shared policy* concerning the hardware and software for VIS and SIS II. This solution, which is referred to throughout the document as a **common technical platform**, deals with locating both systems in the same building (co-housing), connecting them to the same network through a single access point, using the same technological platforms;

2. The development of **common technical platform and services,** dealing with the development of common services between the VIS and SIS II.

The business continuity system will reflect the choices made for the production system.

At the *communication* level, the sharing of a common telecommunication infrastructure was examined.

The impact of these synergies on financial and human resources have been converted/quantified into cost-savings, and documented in the investment and resource planning.

1.4 APPROACH OF THE STUDY

To meet the above objectives and to provide comprehensive answers to the Council conclusions on the guidelines for the introduction of a common system for the exchange of visa data, the study has been conducted according to a top-down approach.

1. Initially, the VIS stakeholders and the supported processes of visa issuance and visa consultation were analysed to determine the required functionalities of the new system (chapter 2);

2. The use of biometrics has been examined from the point of view of providing authentication and identification services, two of the core visa consultation functionalities to be provided by the new system. A range of biometric identifiers (e.g. iris, fingerprints, facial) was analysed using a comprehensive set of selection criteria to determine their suitability in the VIS context (chapter 3);

3. The specifications for the new system have been determined including the functional, technical and operational requirements. Volumes and storage requirements to support the business context, system response times, security measures, system availability and business continuity requirements have been documented (chapter 4);

4. The two main options for the architecture of VIS (see section 1.3) have been examined from a functional, technical and operational angle and to determine the best technical option for the location of the central System C-VIS (chapter 5);

5. Candidate communication infrastructures (e.g. SISNET, TESTA) for VIS have been examined and benchmarked. Connectivity infrastructure requirements between C-VIS and N-VIS, and between N-VIS and offices issuing visas have been determined (chapter 6);

6. The impact on financial and human resources has been reported in the form of an investment and resource plan with an implementation timetable and a multi-annual estimate of

expenditure. Costs are distributed to C-VIS, N-VIS and on the basis of the standard configuration of the consular posts (chapter 7);

7. The solutions for the various options have been compared using a comprehensive set of selection criteria (chapters 8);

8. The VIS system specifications for the central (C-VIS), the national (N-VIS) and for the standard configurations for offices issuing visas have been determined (chapter 9);

9. Lastly the global conclusions and the recommendations of the study have been drawn to aid the decision making process with regard to the VIS (chapters 10);

10. Several annexes complement the main part of the study. In particular:
    - Annex A provides the list of reference documents and abbreviations used throughout the study;
    - Annex B details the VIS business processes and the functionalities of the new system;
    - Annex C describes the possibilities of the integration of the VIS and the integration of the VISION consultation functionality in the future VIS;
    - Annex D describes the role and procedures of the Technical Support Units (TSU) with a view to define the necessary human resources for managing and supporting the operations new system.

2. BUSINESS MODELLING

2.1 INTRODUCTION

Business modelling is a technique allowing organisations to build, analyse and communicate models of their business operations. In the context of the VIS, business modelling aims to define, analyse and illustrate, in the form of simple diagrams, the processes to be streamlined by the new system. The business model enables users of the system to obtain an overview of the processes and functions of the new system from the perspective that is most relevant to them. Business modelling starts with the overall picture of the business to be supported by the VIS system, and drills-down further to the specific processes and their application by the users.

The goals of the business modelling to be employed here are as follows:

1. To reflect on the structure and the dynamics of the organisations involved (stakeholders);
2. To reflect on how the implementation of a VIS could improve the day-to-day operations of the stakeholders;
3. To elicit the functional requirements of the VIS.

Having defined the scope of the business modelling with regards to the new system, the current chapter:

1. Introduces the system stakeholders and the dynamics between them;
2. Describes existing operations and determines the impact of VIS;
3. Documents the business processes and functional requirements;
4. Reveals the key business figures (derived from the stakeholders).

2.2 VIS STAKEHOLDERS

The VIS targets the following organisations and stakeholders (refer to Figure 2-1):

1. *VIS-authorities* in charge of:
   - C-VIS and
   - N-VIS.
2. The *National Central Authorities* of each Member State with responsibilities for visas (operational and organisational competence);
3. *Local Authorities* that are divided into three main users categories depending on the nature of the process they handle:

- Authorities/officials *directly involved* in the *visa-issue procedure*. These are officials at diplomatic missions or consular posts, central national authorities and (in exceptional cases) border crossing authorities;

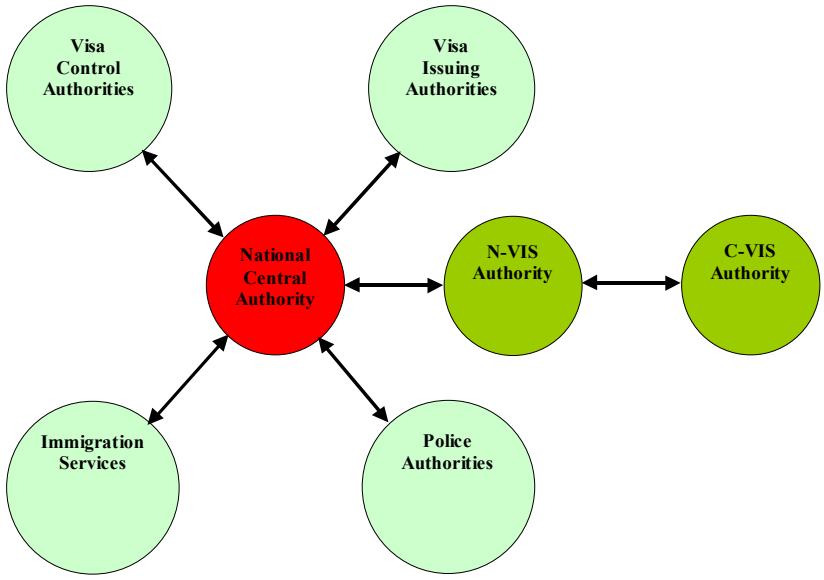
- Authorities/officials *directly involved* in the *visa control procedures*. These are primarily officials at border checkpoints;
- Authorities *indirectly involved* in visa control as part of their day-to-day work:
    - Police authorities operating within the national territory;
    - Immigration services in particular in charge of implementing the regulation replacing the Dublin convention and in charge of returning illegals.

The various responsibilities are undertaken by different administrations at the discretion of each Member State.

In terms of the business dynamics:

1. Local authorities report directly to the National Central Authorities;
2. National authorities oversee the deployment of the uniform rules of the common visa policy at the national level by the local authorities.

Figure 2-1: Stakeholders and their relationships.



2.3 IMPACT OF VIS ON EXISTING OPERATIONS

The VIS will have a significant impact on the organisational structures and the operations of the organisations at the local level.

2.3.1 Diplomatic missions, consular posts

Existing procedures:

Diplomatic missions and consular posts apply the uniform rules laid down in the Common Consular Instructions. In particular, officers in charge of visa issuing:

- Register new visa applications lodged by travellers. Current procedures require travellers to provide the uniform visa application form for a Schengen Visa including a photograph,

their travelling documents as well as a number of supporting documents concerning the planned visit, to enable diplomatic missions or consular posts to ascertain that the applicant is acting in good faith;

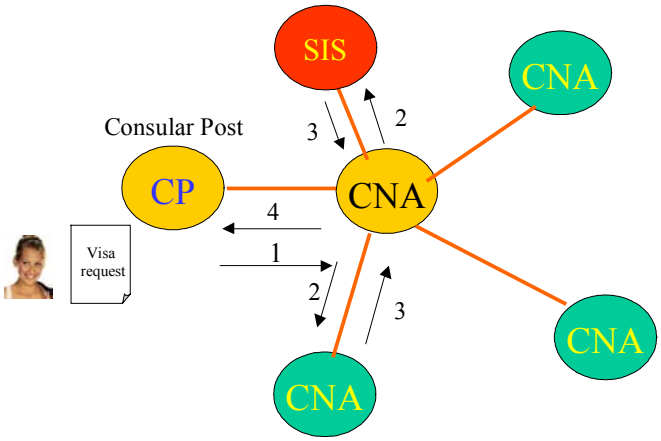
- Examine the visa application including verification of the visa application, the travelling and other supporting documents and consultation of the SIS. These checks are aimed at engendering an improved basis for decisions, ensuring the security of Member States and fighting illegal immigration;
- Supervise the decision making process for visa-issue, in specific cases consulting with the National Central Authority of the Member States, including the VISION consultation;
- Fill-in the visa sticker, and (finally) affix the sticker to the travel documents.

Visa data gathered by the diplomatic missions and the consular posts is stored at the national level. Member States base their visa-issue decisions on information stored at that level, since there is currently no European-wide visa information system.

In exceptional cases, visas can also be issued at border crossing points.

Figure 2-2 depicts a typical visa issue information flow as its is performed today. The consular posts (CP) register the uniform visa data and the photograph. This application is transmitted to the central national authority (NCA) for assessment (1). The national authority consults the SIS in order to determine whether an alert has been issued on the visa applicant (2,3). The VISION consultation is initiated (2,3) for applicants travelling from sensitive countries. The combined results, including the visa issue assessment, are relayed back to the consular post (4), which are in charge of issuing the visa sticker.

Figure 2-2: Visa issue procedure.



Legend:
CP refers to **C**onsular **P**ost
CNA refers to the central national authority

Impact of the VIS:

A new system would have to facilitate:

- The electronic registration of the visa data in an information system to facilitate data sharing among the visa issuing authorities;
- The search and consultation functions to retrieve information from the centralised repository to conduct well-informed visa issuing decisions;
- The improvement of verifications of traveller identities and travelling documents.

New functionality would have to be implemented as follows:

1. Acquisition of biometrics to be subsequently used for verification or identification purposes;

2. Scanning or acquisition of photographs of applicants;

3. Scanning of supplementary documents[3];

4. Assessment of the identification/verification results provided by the VIS system.

Regarding infrastructure, additional technological equipment would have to be installed and maintained, including:

1. Biometric enrolment stations;

2. Document scanners;

3. Secure networking and supporting infrastructure (connecting consular posts to their National Visa Information System (N-VIS)).

Memory chips (aimed at storing visa holder's photograph and biometrics) and chip readers (to be installed at cross-border checkpoints) might be used if this option for the storage was chosen[4].

The new system would have a significant impact on the organisational structures and visa issuing operations. In particular, National Central Authorities will have to work around the clock in order to comply with the response times required for visa-issue (for further explanations see section 2.5.1).

2.3.2 External border checkpoints

Existing procedures:

Border checkpoints assess whether the applicable entry conditions have been fulfilled. They conduct visa and traveller verification for travellers of third countries entering into and leaving the Schengen area. At the present time, traveller verification is performed through visual checks comparing the traveller (carrier of the visa) to the photograph embedded in the passport. Furthermore, SIS is consulted in order to ascertain whether an alert has been issued for the purpose of refusing entry. Visa sticker authenticity is determined by examining its security features.

To make visa sticker controls less prone to fraud, existing legislation mandates the integration of the photograph with the visa sticker. This measure aims to facilitate visual verification between the holder of the sticker and the visa carrier (traveller).

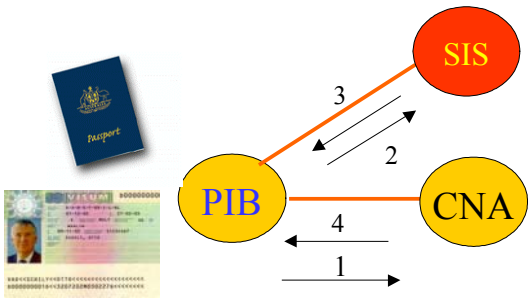
Figure 2-3 illustrates a typical visa control process as it works today. Border checkpoint authorities check the passport and the visa sticker. They determine if an alert has been issued on

[3] In particular passports, residence permits, bank account, residence confirmation letters, insurance and airline tickets.

[4] This option which is linked principally to the development of the visa sticker was not part of the Council requirements and therefore has not been assessed in this study.

the traveller in the SIS (2,3) and they consult with the central national authority in implementing the national measures (1,4).

Figure 2-3: Visa control.



Legend:
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
CNA refers to the central national authority

Impact of the VIS:

The VIS would introduce another layer to the verification of bona fide travellers as well as to the fight against fraudulent visa stickers and fraudulent claimed identities. It would utilise biometric technologies to support accurate traveller verifications, if so decided by the Council. Validation of the visa sticker would be performed by comparing the visa sticker of the traveller to its image stored in the VIS database. Similarly, the traveller's identity would be compared to the identity of the person to which the visa has been issued (in order to confirm that the carrier and the holder are one and the same person).

VIS would also have a substantial impact on the procedures and supporting infrastructure for checking travellers, particularly deriving from the use of biometrics. This impact also includes the need for necessary training of staff, and the costs associated with these activities. In particular, capital investments include procurement and installation of the biometric acquisition and processing equipment as well as setting up the communication infrastructure between the border checkpoints and the national visa information system (N-VIS).

2.3.3 Police and Immigration authorities

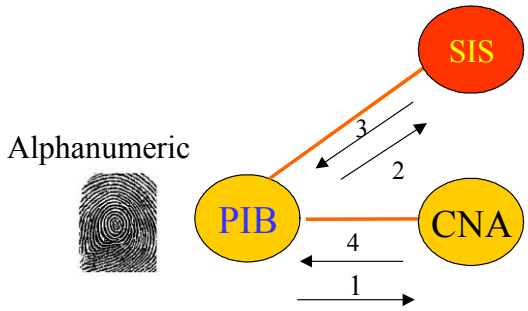
Existing procedures:

Police checkpoints are set-up by the Member States in order to improve internal security and to combat terrorism. Police authorities conducting the controls (checks) are required to accurately verify the identities of documented aliens and to identify undocumented aliens.

The Immigration Services of the Member States are also involved in the verification of documented aliens as well as the identification of undocumented aliens, The verification and identification processes including retrieval of supporting documents would facilitate the return of illegal residents to their countries of origin and the determination of the state responsible for examining an asylum application in accordance with the Regulation replacing the Dublin Convention.

Figure 2-4 illustrates a typical person-identification process as it works today. Police authorities acquire biometrics or other data carried by the person in question in order to make a determination of identity. They verify whether an alert has been issued on the traveller in the SIS (2,3) and consult with the central national authorities.

Figure 2-4: Person identification.



Legend:
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
CNA refers to the central national authority

Impact of the VIS:

From a business perspective, police and immigration authorities could use VIS for verification and identification purposes. The introduction of these new capabilities would require the budgeting of significant training activities.

This translates to capital investments as these authorities would need to be equipped with and trained in the proper use of the necessary biometric acquisition and processing devices connected to the VIS system.

2.4 VIS BUSINESS PROCESSES

With regards to the previous business context, VIS targets the automation of two core business processes: **visa-issue** (done at diplomatic missions, consular posts, National Central Authorities and exceptionally at border crossing points) and **VIS consultation** (done at the border control and other police or immigration checkpoints).

The **visa-issue** process deals with visa application and visa applicant *registration*, visa application *assessment* and the management of the visa issuing *decision*. Supported functions include:

- Electronic registration of the visa application;
- Enrolment of the visa applicant (including photograph and biometrics);
- Negative identification[5] of applicants not in possession of an old visa sticker;
- Verification of an applicant in possession of an old visa sticker (e.g. bona fide traveller) using the visa sticker number;
- Information on whether a previous visa application was refused, revoked etc…
- Consultation of National Authorities, including the actual VISION consultation;
- Management of the visa application status (granted, refused etc...).

The **VIS consultation** process supports verification of visa applicants or other documented aliens, as well as identification of undocumented aliens with the purpose of returning aliens

[5] Negative identification verifies that an applicant is not already enrolled in the VIS database with a different identity.

(either "illegals" or asylum-seekers) to the appropriate country. Visa consultation could also be used to authenticate a visa sticker and the visa carrier at cross-border checkpoints (and eventually verify that the carrier and the holder of the visa are the same person). Supported functions include:

- Verification of aliens in possession of a visa sticker;
- Identification of aliens not in possession of a visa sticker;
- Documentation of an identified alien (name, nationality etc...) and
- SIS consultation.

Figure 2-5 illustrates the visa-issue process initiated when a new visa application is lodged at a diplomatic mission or consular posts: Visa application registration and processing, assessment (consultation) and visa-issue decision.

Figure 2-5: Visa-issue process.

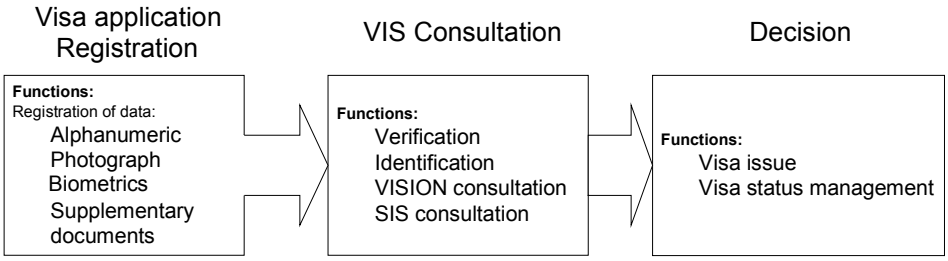


Figure 2-6 illustrates the VIS consultation process.

Verification is performed during visa-issue and at cross-border checkpoints to check the authenticity of the visa sticker and to verify that the carrier and holder of the visa are one and the same person.

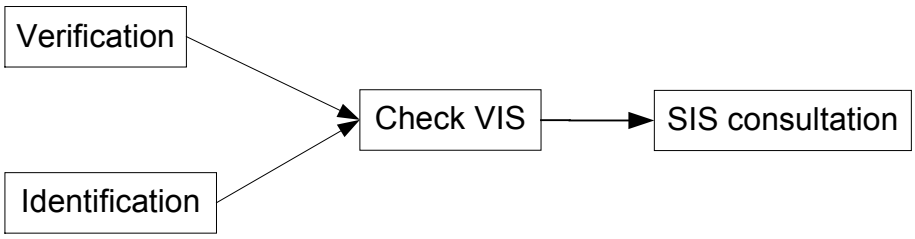
Identification is applied at cross-border checkpoints as well as by the appropriate police and immigration authorities in order to identify undocumented persons.

Verification is a two-step process in which the first step involves a claim of identity that is subsequently followed by determination of the validity of the claim. The verification is actually a comparison between the *"claimed identity"* and the *"true identity"* as stored in the VIS. The claimed identity is used as the key to retrieve information from the system to verify the claimed identity. From a technology perspective, verification is a **one-to-one** database search; it does not require large amounts of computing power and is not an expensive process (in monetary terms) to implement.

Identification is the process of determining a person's identity. It involves the comparison of some unique trait of a person (e.g. an inherent, captured, and field-measurable biometric[6] trait) with templates of the same trait, in search of a possible match. From a technological perspective, identification is a **one-to-many** database search, requires a significant amount of computing power and it is an expensive process to implement.

[6] The use of biometrics is analysed in chapter 3.

Figure 2-6: VIS consultation process.



The VIS system could facilitate the SIS consultation as part of the VIS consultation process.

With regard to the previously described processes, and with typical in-the-field applications of the VIS in mind, the new system could integrate the following business processes:

1. Visa-issue:

    a) New visa without previous registration (referred to as "Visa/applicant registration without a previous VIS registration");

    b) New visa with previous registration (referred to as "Visa/applicant registration with a previous VIS registration");

    c) VISION consultation, to implement the consultation between the central authorities of the Member States.

2. VIS consultation:

    a) Visa and traveller verification (at cross-border checkpoints);

    b) Person identification (by police and immigration authorities);

    c) SIS consultation, to verify whether an alert has been issued on the applicant in the Schengen Information System (SIS);

    d) Possibly existing national systems.

These business processes[7] will constitute the basis for the quantitative model and the subsequent sizing of the system.

Reporting and statistics will be supported as a management process of the VIS system. Nevertheless this process will not significantly affect the sizing of the system, since the impact will be negligible compared to the other four business processes.

The proof-of-concept concerning the VIS business processes is illustrated in the table below which maps VIS objectives to the VIS business processes.

[7] For detailed analysis of the business processes, refer to Annex B herein.

Table 2-1: VIS objectives –Business Processes Matrix.

Business Process	Fight fraud (a)	Improved co-operation (visa authorities) (b)	Facilitate checks (c)	Visa shopping (d)	Dublin Convention (e)	Return Illegals (f)	Common visa Policy and towards internal security and combating terrorism (g)
Visa/applicant registration without a previous VIS registration	✓	✓	✓	✓			✓
Visa/applicant registration with a previous VIS registration	✓	✓	✓	✓			✓
Visa and traveller verification	✓		✓		✓	✓	✓
Person Identification	✓	✓	✓		✓	✓	✓

2.5 BUSINESS FIGURES

Diplomatic missions, consular posts as well as the National Central Authorities of the Member States are involved in the handling and management of visa applications. The assumption has been made that the capacity to process 20 million visa requests per year will cover the global needs during the next five years. This figure includes the Member States and the accession countries as well as Norway and Iceland, which participate in the Schengen co-operation. The figure has been computed by extrapolation of the current visa statistics (12 million visa requests per year) provided by the participating countries. It is assumed that 20% of the visa applications are lodged by frequent travellers already enrolled in the VIS. It is also been assumed that 20% of the total visa requests are subject to VISION consultation between the National Central Authorities of the Member States. Finally the figures assume a SIS consultation for every new visa request and visa control.

Considering the total number of visas issued yearly and the number of multiple-entry visas included therein, cross-border checkpoints (in charge of visa control) would have to perform 40 millions visa and traveller verifications per year (taking both entries and exits into account). Finally, it has been estimated that the actions of police and immigration authorities in charge of identifying undocumented aliens would add another 5 million person-identifications to the system per year. Table 2-2 provides a summary of the business figures concerning the VIS system. These figures are the basis for determining the storage and bandwidth requirements. Note that an additional 20 million SIS consultations will be introduced as part of the visa issue process. This does not impact the VIS but rather the SIS, and hence, reported separately.

Table 2-2: Key business figures.

Visa issue (consulates and national central authorities):	***20 000 000***
New visa with previous registration	4 000 000
New visa without previous registration	16 000 000
VIS consultation:	***45 000 000***
Visa and traveller verification (entry plus exit at border checkpoints)	40 000 000
Person identification	5 000 000
Other consultations:	***4 000 000***
VISION consultation	4 000 000

SIS consultation (visa issue, entry and exit)	60 000 000

2.5.1 Schedule of operations and system use

The VIS functions are available to the users 365d/7d/24h. In order to estimate the load generated by each category of users at peak moments, the following operational assumptions have been made:

1. Diplomatic missions or consular posts handling visa applications are located world-wide, working according to a standard 8-hour schedule. They make use of the VIS system 24 hours a day because of the different time zones;

2. National Central Authorities of the Member States involved in the visa-issuing consultation process work on a 7d/24h schedule in order to comply with the response time requirements;

3. Cross-border checkpoints in charge of visa control operate during extended working hours, seven days a week. They mainly use the system during a 16-hour day;

4. The immigration authorities and police authorities dealing with immigration issues mainly use the system during normal working hours. The system is used seven days a week.

Figure 2-7 illustrates the volumes contributed by the various processes.

Volumes for new visa request: Visa requests are primarily handled by consular posts and to a lesser extent by the National Central Authorities. Due to their world-wide locations, the volume contributions are constant during a three-day window (all the countries are operating). The remaining four days reflect the weekend-effect where volumes are decreasing.

Volumes for person identification: Person identification contributes a symmetric weekly pattern, constant during working hours.

Volumes for visa and traveller verification: Visa and traveller verification contributes a symmetric weekly pattern also constant during working hours.

Figure 2-7: Weekly pattern of the average arrival rates.

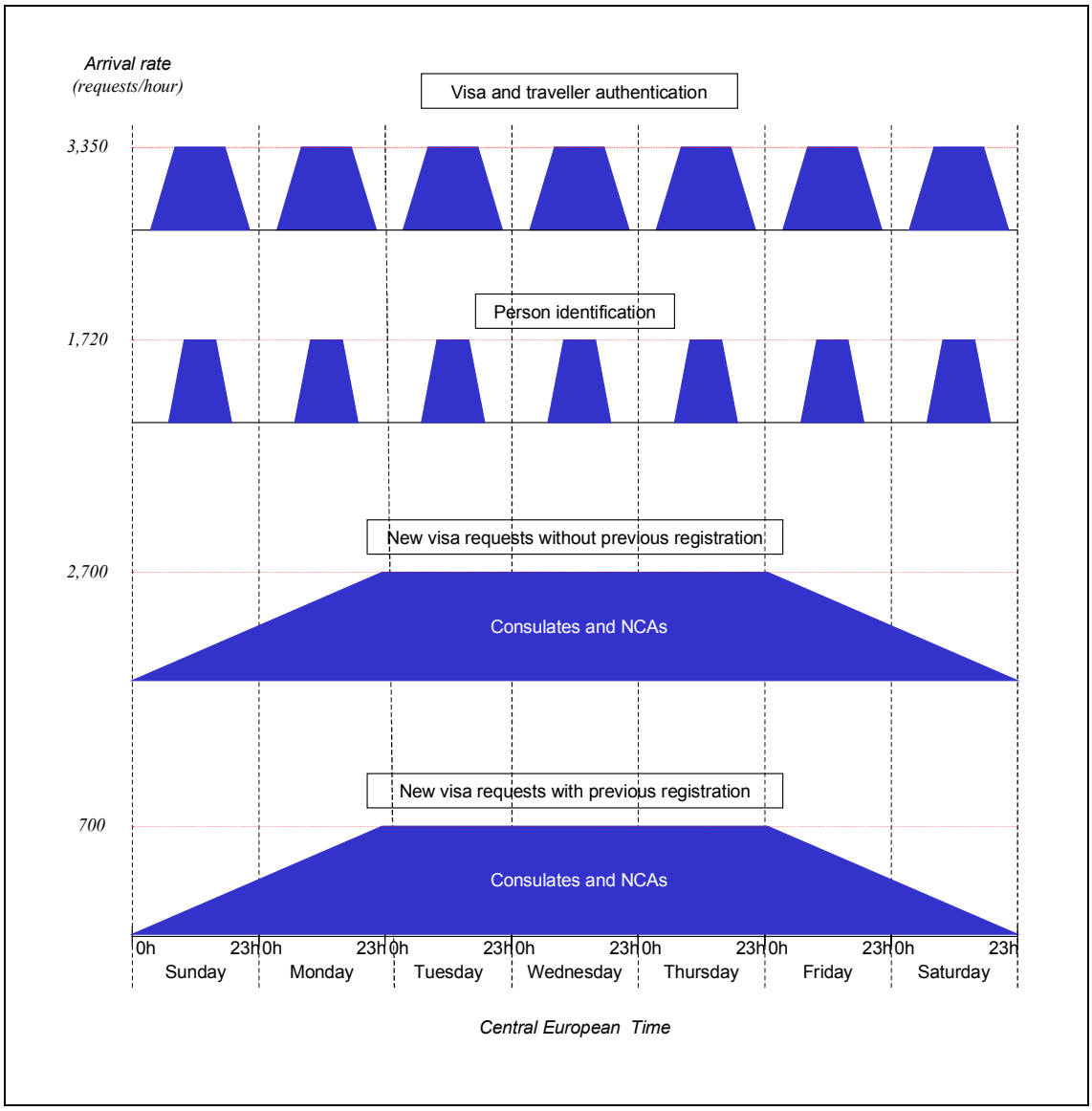


Table 2-3 displays the arrival rates of requests to the various VIS processes when considering the key business figures of Table 2-2. An example of a typical computation reads as follows:

- The business figures stipulate that the system should support 5,000,000 person identifications per year;
- The system usage depicted in Figure 2-7 shows that police and immigration authorities query the system equally often, during 8-hour timeslots, everyday;
- Therefore, the peak usage for the person identification process (in requests per hour) is computed as follows: $\frac{5{,}000{,}000}{8 \times 7 \times 52} = 1{,}720$ requests/hour.

Table 2-3: Average requests arrival rates.

Process		requests/hour	requests/sec.
New visa	without previous registration	2,700	0.75
	with previous registration	700	0.2
Person identification		1,720	0.5
Visa and traveller verification		6,700	1.9

These arrival rates have been used in chapter 6 to derive the transaction rates and network bandwidth requirements to meet the response times.

2.6 CONCLUSION

It might introduce *technical* and *operational* changes as well as *new procedures* into the target organisations. These changes are essential in order to meet the objectives as stated by the Council (refer to Table 2-1).

The new system will necessarily incur training costs associated with the changed procedures, the new system functions & equipment and in particular the use of biometrics.

New information flows would have to be created as a result of storing and sharing the visa data between the Member States, including photographs and biometrics. One consequence of the introduction of the new system would be the adaptation of existing procedures or the introduction of new procedures.

The work of the *Visa-issue authorities* would have to be facilitated via the necessary upgrading of the technical and communication infrastructure, and by engaging additional human resources to execute the new procedures to be introduced by the VIS. The technical infrastructure would include biometrics acquisition devices and scanners as well as the communication infrastructure. New procedures would include the acquisition of biometrics, the electronic registration and management of the visa data, and identification of travellers.

Similarly, the work of *visa control* authorities would be facilitated via technical and communication infrastructure upgrades needed to consult with the VIS system to verify the identity of the travellers and the authenticity of visa stickers. New procedures would include the acquisition of biometric data and consultation with the VIS.

Police and immigration authorities should further consider connecting to the VIS system to make use of the biometric-based identification functionality. Likewise, the work of these authorities would similarly be facilitated via the necessary upgrades to the technical and communication infrastructure. New procedures would include the acquisition of biometric data and consultation with the VIS.

3. BIOMETRICS

The purpose of the biometrics section is to select a few candidate biometric systems that match the VIS needs. Recommendations will then be made so as to proceed to a final selection.

3.1 INTRODUCTION

Biometric data are large numbers derived from *measurements* (called biometric samples) of either **physiological** traits (part of a person's anatomy) or **behavioural** traits (action performed by a person). Such traits are also simply called biometrics whilst the formatted numbers are known as biometric templates. The actual list of all possible biometric identifiers is a long one and probably to date not completely identified. However, only five of them, which are in competition with each other, currently receive industry support and will be considered:

- **Fingerprint**. This is based on the distinctive features of fingertips, called *minutiae*. A surface finger is placed on a glass and scanned in order to capture a high-resolution picture of the tip, which is then processed in order to extract the minutiae locations, and then recorded in a template. Flat or rolled fingerprints can be acquired. A rolled fingerprint requires rolling the finger from one edge of the nail to the other and will reveal more minutiae than a flat fingerprint. Thumbs and the indexes are the fingers with the most informative content. The various fingers of a same person are different and uncorrelated;
- **Face**. This is based on the more permanent features of the human face like the upper outlines of the eye sockets, the distance between the eyes, the areas around the cheekbones and the sides of the mouth. They are extracted either from black-and-white or colour, high-resolution, pictures. Using photographs as a source for face recognition implies certain quality requirements and a standardised manner of taking the photographs;
- **Iris**. This is based on the many distinctive features of the iris (the coloured ring that surrounds the pupil). An infrared ray of light scans the eye and a camera captures a high-resolution black-and-white picture of the iris, which is then processed to extract the iris features and stored in a template. This capturing process is rather quick and could be considered as contactless. The technique is said to be safe provided that the capturing devices are maintained correctly. The two irises of a same person are different and uncorrelated;
- **Hand geometry**. This is based on measurements of the hand's distinctive features like finger height, width and length, as well as the distances between joints and knuckle shapes. The hand is placed flat on a metal surface where pegs guide the fingers into position. Then two pictures, one of the back, the other of the side, are captured and further analysed to extract the hand features;
- **Retina**. This is based on the distinctive features of the patterns of blood vessels found on the thin nerve on the back of the eyeball. A ray of light scans the eye and a camera captures a black-and-white, high-resolution, picture of the retina, which is then processed to extract the retina features and stored in a template. It is a longer and more difficult process than the four previous ones since it requires a higher level of co-operation.

The basic feature of biometrics is to allow to *uniquely* link a biometric template to a specific person. Therefore a biometric identifier is basically an **identifier** that can prove who you are in the same way photographs have been used to do so for many years (think of identity cards, driver licenses and passports). In this sense all traits that are unique to each individual might be used to derive biometric templates.

3.1.1 Biometrics uses

The procedure of acquiring biometrics and storing them is called **enrolment**. In order to avoid enrolling the same person twice, the enrolment procedure will systematically perform an identification before taking the decision whether to store a new record or not

A biometric system can check individuals along two distinct modes depending on the information available:

1. The **identification** mode works on the basis that no 'identity' is assumed. This is done by comparing a person's biometric identifier with the biometric identifiers of all other persons stored in a database in order to find a possible matching identity. This is a **one-to-many matching process, and is thus computer intensive;**

2. The **verification** mode checks a person's claimed 'identity'. This is done by comparing a person's biometric identifier with that of one associated with the name claimed by this person. It is a simple **one-to-one matching process, and is thus not a computer intensive process**.

Since identification requires performing as many comparisons as there are number of cases in the database, compared to a single comparison for verification, **identification costs are much higher than verification costs.**

3.1.2 Biometrics in the context of VIS

Biometrics, as verification and identification means, are part of the toolbox expected to help reach the strategic objectives of the VIS. Understanding the business context will help to select the most appropriate biometric identifier for the VIS.

Biometrics apply to the VIS business processes in the following way:

1. **Visa issuing without previous registration.** A negative identification is performed each time a visa requester is not in possession of a previously issued visa. The purpose of negative identification during the visa issuing process is to avoid enrolling in the VIS database a same person under two different identities and visa histories. In other words a 1:many comparison is being launched in order to check if a person has already applied for a visa under another identity.

2. **Visa issuing with previous registration.** When a visa number is available, it is used as a key to directly retrieve the visa requester's history in the VIS database. A 1:1 comparison should confirm that the person is still the same one as the person who previously applied for a visa.

3. **Visa and traveller verification.** Verification of visa carriers is performed at external border checkpoints, police departments and immigration departments of MSs. The verification (1:1 comparison) should prove that the visa carrier is the same person as the visa holder (i.e. the person to whom the visa was actually granted). The current procedure uses the photograph to visually check the visa carrier. Biometrics can greatly increase the reliability of the control procedures and could even be partly automated in airports and seaports by setting up specifically equipped gates.

4. **Person identification.** Positive identifications are performed by police and immigration officers, possibly after a failed verification or if the person is completely unknown. The

identification should help officers document aliens with a view to possibly deport them to an appropriate country or to confirm that the person has legal permission to stay.

There is no alternative for identifying undocumented persons.

Biometrics are a powerful complement to alphanumeric data like name, nationality or age for searching though a huge database like the VIS. Searches based on alphanumeric data alone will for e.g. provide many matches for common names such as "Miller", "Dupont", "Singh" or "Mohamed", this implies that searching one of those names could return up to 50 hits for instance. Such a high number of possible cases makes it virtually impossible to identify the person who is to be checked. With sufficiently accurate biometrics, the reliability of the identification procedure as well as its speed would dramatically improve (of an indefinite number of persons, only the person to be checked would be retrieved from the database and thus identified). Moreover, it would allow a more flexible name search, which may prove to be useful in order to avoid situations where difficulties could arise, such as when names are misspelled or just written in a different way (e.g. is "Gerald R. Smith" identical with "Gerald Smith") and therefore minimising transliteration issues.

3.1.3 Biometrics accuracy

Two biometric measures of a same person are never identical due to the variations in environmental conditions (scanning device, temperature, humidity, light, etc.) and the enrolee's attitude during the enrolment process. Although the technology is constantly improving, two types of errors are still possible:

1. *Accepting a match that is wrong*, i.e. granting a person the identity of somebody else enrolled in the biometric database. This is called a **false match**;

2. *Rejecting a match that is right*, i.e. not recognising a person who is enrolled in the database. This is called a **false non-match**.

Basically these two types of errors are sensitive to the following factors:

- The probability of false non-matches increases as the acquisition conditions vary between enrolment, verification and identification processes;
- The poorer the acquisition conditions, the higher the probability of false matches;
- In identification mode, the larger the database, the higher the probability of false matches.

This last point is of particular importance in the case of **VIS,** since it **will operate the world's largest biometric database**, (even larger than the FBI's, which stores more than 40 millions records).

Accordingly the level of accuracy of a candidate biometric identifier should be high enough to reduce errors to an acceptable level.

3.1.4 Biometrics sensitivity

Biometric images and templates can be compared to passwords since they carry the same functionality. Accordingly a **stolen template** could allow someone to acquire someone else's identity for life (biometrics cannot be replaced once they have been stolen) and this in every system using this biometric identifier. For this reason all biometric templates need, from their

creation, to be secured in the capturing device in order to minimise the risk of manipulation or uncontrolled access.

3.2 OVERVIEW OF BIOMETRICS

Section 3.1 has highlighted five possible biometric identifiers that have to be compared in order to make an appropriate choice for the VIS. Accuracy and system costs are not the only elements to be taken into consideration in order to compare biometric identifiers, indeed, other *limitations* do exist.

The major limitations of biometrics are briefly introduced hereafter and will lead to the pre-selection of a few candidate biometrics. In order to further compare the candidate biometrics an overview of the market maturity is reported in section 3.2.2.

3.2.1 Limitations and problems of biometrics

The following outlines the most common criteria used to compare biometric identifiers:

1. Acceptance:

The choice of a biometric identifier should take into account the enrolment procedure's acceptance of the enrolee population. Acceptance rate might be lowered due to the following:

- **Privacy** concerns; uses could be broader than intended purposes e.g. law enforcement, surveillance or health diagnosis (see biometric sensitivity);
- Fear of **intrusive** acquiring devices that might annoy or injure enrolees;
- Acquiring devices that require physical contacts could raise **hygiene** concerns;
- **Religious or cultural peculiarities**.

All biometrics will face a certain extent of acceptance problems. **In the case of VIS, visa applications from persons refusing to provide their biometric identifier might simply not be considered.** Experiences with existing civilian systems that provide benefits such as travel authorisation or election registration for the enrolee have shown that the refusal rate is low.

2. Suitability:

Between 1 and 3 percent of the general public do not have the body parts (or sufficient body part quality) required for mapping any biometrics with the exception of face.

A *fallback system* should be considered for persons who cannot enrol through the system's main biometric identifier. This fallback system could be the current procedure or another biometric identifier. In order not to create a security breach in the VIS system, the fallback system should ideally feature the same level of accuracy as the main biometric in both verification and identification modes.

3. Uniqueness:

The purpose of biometrics is to uniquely identify individuals. In the case of a very large database like VIS (70 millions records), one needs a biometric identifier that has proven to be unique for such large populations.

4. Stability:

The biometric identifier should be stable (constant) during the period of its usage by the system. Unstable biometric identifiers will lead to increasing false non-match rates over time:

- Whereas the structure of fingerprints is rather stable over a life span, fingerprint sizes can grow between childhood and adulthood. Special computer matching algorithms are being developed to take this into account;
- Face recognition techniques are subject to instabilities introduced by people intentionally changing their facial characteristics or as a result of the ageing effect. It is commonly admitted that facial features become unstable after 18 months;
- For the iris it is assumed that the structure is stable over the whole life span. Contrary to fingerprints, where lifetime stability has been proved, iris biometrics is rather young and therefore, for the time being, one has to rely on scientific estimates;
- With regards to hand geometry, it is known fact that the geometry changes over time. As for retina, one can refer to the iris since they follow the same pattern.

5. Robustness (misuse):

Robustness deals with counterfeit input data to a biometric verification/identification system. Counterfeiting can occur in two ways:

1. When an attacker presents a stolen *biometric identifier* (false fingerprint or voice recording for example). This is known as the "liveness issue";

2. When an attacker replaces a trial or reference *template*. This is known as an electronic attack.

The existence of electronic attacks has been known for many years and has attracted much attention with the growth of the Internet. Some specific cryptographic techniques can be carefully applied to avoid such a risk. All biometrics are equally exposed to electronic attacks. Liveness attacks are dealt with through counter-measure techniques implemented in scanning devices. However, this risk can be minimised if the enrolment process and the verification process are supervised and as little as necessary room and time is left for unsupervised manipulation.

6. Enrolment/acquisition conditions:

Acquisition conditions (scanning device, temperature, humidity, light, enrolee attitude, age, etc.) are crucial for the quality of the images and templates and consequently for the accuracy of the system, in particular for improving the false non-match rate. Therefore acquisition environments should comply with acquisition requirements as much as the operational conditions permit (consulates, cross-border checkpoints, police and immigration offices). Hence **biometric identifiers' sensitivity to acquisition conditions should be assessed in the context of VIS (consulates and cross-border checkpoints)**.

7. Enrolment/acquisition procedure:

As some biometrics require complex acquisition procedures, supervision may be needed to some extent. Operational impacts of supervision have to be considered:

a) The **acquisition time** will directly translate into personnel costs and additional investments to cope with queues, particularly when several attempts are necessary to get an acceptable sample;

b) The level of required **technical expertise** from the personnel should be reasonable in order not to increase training costs too much.

8. Accuracy:

The issue of accuracy has been outlined in section 3.1.3.

9. Failure-to-enrol rate:

In order to improve the quality of the biometric database some systems perform a quality check during the acquisition procedure and reject people with poor biometrics. This results in improved accuracy on the one hand and to a fraction of the population not able to enrol with the system (similar consequences as user unsuitability) on the other. Accordingly **the accuracy of a system should be considered jointly with its failure-to-enrol rate**.

10. Response time:

A biometric system should be able to guarantee response times in compliance with the business requirements. As matching operations are well suited to parallel computing techniques it is always possible to increase the transaction speed to the required level. Hence response time is a matter of cost.

11. Storage:

Images and templates can either be stored in central or local databases or even on portable devices (like chip cards). The size of images and templates is not critical for storage systems that are scalable. However, the storage requirements need to be assessed when considering storing images or templates on devices with limited storage capacity. The current limitations for such devices are:

- Scanning devices (a few Mbytes);
- Chip cards (less than 512 kbytes for pure contactless memory cards) and
- 2-D barcodes (1.1 kbytes).

Storage of images will require much more space than that of templates, however, as the coming sections will outline, it will ensure a better interoperability between vendors. As a general rule, we can say that 2-D barcodes can only store templates, while chip cards offer enough room to store images whatever the type of biometric identifier is. Nevertheless, the technology is still evolving rapidly and a growing storage capacity for all kind of devices can be anticipated.

3.2.1.1 Pre-selection of candidate biometrics

In the VIS context, choosing a unique and stable biometric identifier is the key-requirement. This automatically disqualifies face and hand geometry as the main biometric identifier. Although retina provides the required uniqueness and probably the necessary stability features, it scores poorly on accuracy and thus it is not suited for the VIS (a very large database).

From the remaining two identifiers iris and fingerprints could be used as a primary biometric identifier in the context of a large VIS database. Both of them provide a high level of accuracy (not yet proven in practice for iris) and therefore could be suitable for the required verification and identification processes. For those persons who are not able to provide sufficient biometrics, a fallback procedure is required. This could take the form of face recognition with the risk of low accuracy or the manual comparison process of comparing personal appearance and a

photograph travel document (and/or visa) photograph as it is done today. Such photographs could also be, either printed, and/or electronically stored on the appropriate document.

Fingerprints, iris and face will be compared in section 3.3.

3.2.2 Biometric identifiers and market maturity

The VIS candidate biometric identifiers (fingerprints, iris and facial) should also be examined with regards to their market maturity. The choice of a product and vendor should provide certainty about:

- The *permanence* of the system: can we be confident that the maintenance and upgrading of the system will be possible for many years to come?
- The *performance* of the system: can we be assured that once set up, the system will operate with the expected accuracy, speed and reliability?
- *Interoperability* between system components: can we mix hardware and software stemming from various vendors into a single system?

The permanence of the system will be enhanced if several interoperable vendors compete on the market. Interoperability requires availability of standards, which are rather limited nowadays. Accordingly, a higher interoperability between vendors could be reached by using established standards rather than using proprietary data formats that belong only to one single vendor. The performance of the system can only be proven if similarly scaled systems exist and that objective **performance benchmarks** are available or can be organised. Unfortunately such benchmarking results are not yet available for all biometric identifiers under consideration. Even available independent benchmarks suffer from the following drawbacks:

- They cover small databases and do not provide statistically representative results;
- They run on small hardware configurations and do not compare to VIS transaction rate requirements;
- Acquisition conditions comply with a methodology that does not necessarily match the VIS operational conditions. Therefore accuracy, failure-to-enrol rate and acquisition time might be different in the context of VIS.

A biometric identifier that cannot offer sufficient guarantees for permanence and performance should be rejected in favour of a proven one that meets the VIS requirements.

3.3 CANDIDATE BIOMETRICS COMPARISON

This section gives an overview of the candidate biometrics in order to compare them and to derive possible configurations that could satisfy the VIS requirements.

3.3.1 Face

Face as a biometric identifier offers three very attractive features: it is not intrusive, it is easy to acquire and it is available from any human being. The algorithms currently used for facial recognition are based on features that are not very stable over time and that vary depending on the head position, face expression and features (hats, hairstyle, eyeglasses, beards, etc…). Facial recognition, especially for identification purposes, is also very sensitive to the lighting conditions. As already mentioned, the accuracy of facial recognition is poor, and independent

benchmarks simulating operational conditions have even shown far less accuracy than claimed by vendors.

The major consequence of this lack of accuracy results in the inappropriateness of facial recognition to cope with identification against large scalable databases. This excludes facial recognition to be used as a primary biometric identifier. However, in the case of VIS, the face could be used to support the verification process. This verification could either be supported by computer aided comparison, if a benefit is seen in this, or simply done by visual comparison of a person with the photographs as it has been done up to now.

Depending on the technical developments in the multi-model biometric comparison field, an encoded photograph could be used for second level matching processes at a later stage.

As regards market maturity, the market for face recognition is still fragmented and small. Only two leading vendors currently provide large scale databases for faces. Due to the attractive features mentioned, face recognition is receiving more and more attention to in the biometric industry, which should lead to improvements in accuracy and a larger base of vendors within the next ten years.

Till then, computerised facial recognition does not seem to have any additional value for the VIS processes. Nevertheless, depending on the technical developments in the multi-model biometric comparison field, photographs could be encoded and used at a later stage for e.g. computerised second level matching when the technical developments and the market maturity have improved.

3.3.2 Fingerprints

Fingerprint technology is the oldest and most mature identifier and is already used in all Member States. Its high accuracy has been proven by the largest identification systems worldwide (such as the FBI law enforcement system, which stores more than 40 million records). Other large-scale projects are being implemented such as the Malaysian ID card (approx. 20 mio cards), the Philippines social security card (5 mio. Issued on a total of 35 mio. cards foreseen), the Nigerian ID card (60 mio. cards to be issued), and so forth. In the case of VIS, fingerprints could be used for verification and identification as the primary biometric identifier.

Currently, for very large systems, only four suppliers compete, among which, one European company. The market offers guarantees for permanency.

It is currently being considered whether SIS II will implement a biometric identifier storage and/or query system. Given the police context of SIS II, there is a certain likelihood that one of the biometric identifiers to be used with the SIS II will be fingerprints. As the SIS is always consulted during the visa issuing procedure and at border control, the biometric identification feature of SIS II and VIS could lead to important synergies (see chapter 5), **provided that the VIS system chooses fingerprints as the main biometric identifier as well**.

So far fingerprints are appropriate to all of the VIS business processes as the primary biometric identifier.

3.3.3 Iris

Iris technology is quite new (developed as from 1992) compared to fingerprint identification, but seems to be the only biometric able to compete with it when considering large scalable

databases. Iris promises to be far more accurate and faster than fingerprints but has not proven this capability with very large systems, since the largest one counts less than one million records whilst the largest independent benchmark has been performed on a database of only 128,000 records.

As regards market maturity, all the patents (including a patent on the concept) are held by a single U.S. company, which in turn licenses the algorithms to other companies. This single company acts as a licenser to the application and hardware developers, manufacturers and integrators. Therefore a system can be supplied and maintained by several vendors, while a license fee for the algorithm has to be paid to this single company.

No standards exist for iris and interoperability due to the uniqueness of the algorithms (including encryption) from one single company.

The use of iris as biometrics identifier might improve the VIS business processes but does not support the objectives of the Council. In particular the use relating to combating terrorism is rather doubtful because currently there are no well-established iris databases available that could be used for background checks. Moreover criminals or individuals do not leave an iris mark on crime scenes. Finally, the patent issue, lack of operational experience with large-scale databases and an immature market leads to discarding iris as a potential biometric identifier for the moment.

3.3.4 Candidate biometrics comparison (table)

Considering the future size of the VIS database, only fingerprints provide a proven, high level of accuracy. As regards iris, for the moment the market is not mature enough and the scientific accuracy calculations have not as yet proven sufficient guarantees of permanence in operational large-scale systems. Even if things improve in the years to come, a near-future implementation would require discarding iris and leave fingerprints as the unique current option. All three biometric identifiers under consideration (fingerprints, iris and face) can be used for verification, but we do not see any reason to further consider iris if fingerprints is kept as the biometric identifier. The situation is summarised in Table 3-1 when considering the appropriateness of a biometric trait to the VIS business processes.

Table 3-1: Appropriateness of biometric identifiers to the VIS business processes today.

	I)	II)	III)	IV)
	Visa issuing without previous visa registration	**Visa issuing with a previous registration**	**Visa and traveller verification**	**Person identification**
Fingerprints	Yes	Yes	Yes	Yes
Iris	No	No	No	No
Computerised face recognition	No	No	No	No

3.3.5 Recommendations

According to the previous analysis the recommendations are as follows:

1. Fingerprints should be used as the primary biometric identifier in both modes, i.e. identification and verification;

2. Facial recognition systems should not be used for the moment. Since a photograph would be necessary at any rate, the photograph should be taken digitally and in a uniform manner, complying to common standards so that they can be used for computerised facial recognition at a later stage. One should not invest in IRIS or other biometric technology as long as these new technologies are not proven. Given the number of embassies, consulates and entry/exit points, the risk for such a huge investment in both monetary terms and resources would be very high. Iris recognition might be further developed later on and the market maturity might reach a reasonable level;

3. In order to improve the accuracy in identification mode, the application of filtering on the VIS database prior to a biometric search is recommended. Filtering is all about using available and reliable information, e.g. the sex and age ranges of the person to identify, to reduce the size of the set of records to be searched in the biometric database. Filtering should lead to searching only in a certain part (e.g. 10%) of the VIS database for each identification.

3.3.5.1 How can fingerprints be used for each of VIS processes:

I) Visa issuing without previous registration

A ten-finger image (flat prints) would be obtained from the applicant if he/she applies for a visa for the first time. This image would be submitted to the central system for:

1. Storage;

2. Negative identification to be sure this person did not apply for a visa before under a different name.

The reasons for using 10 fingers are:

a) It is easier and more reliable to capture ten fingers rather than selecting various specific fingers;

b) Capturing specific fingers would require more supervision and in some cases physical contact from the consular officers with the applicant;

c) Remaining fingers can still be used for comparison if other fingers are temporarily damaged and therefore not available;

d) Having all ten fingers available will allow background checks against other databases such as national databases or international databases (e.g. SIS II), whatever the number of fingers used in those fingerprint databases is;

e) The VIS database would support latent searches (combating terrorism);

f) The risk of insufficient accuracy can be minimised (see “note” below).

II) Visa issuing with previous registration

A ten-finger image (flat prints) would be obtained from the applicant so as not to change the fingerprints taking procedure. The necessary number of fingers would be submitted to the VIS biometric engine in order to confirm that the applicant is the one to whom the VISA has been previously issued (verification).

III) Visa and traveller verification

The necessary number of fingers (flat prints) (see "note" below) would be submitted to the VIS biometric engine in order to confirm that the applicant is the one to whom the VISA has been issued (verification).

IV) Person identification

In the case of a person identification, ten fingerprints (flat prints) would be obtained and submitted to the central system for identification.

Note: The number of fingers necessary to produce a match depends on the size of the database (number of persons). As no reliable figures regarding the accuracy of fingerprints in a 70 million fingerprint record database are currently available, and considering the high cost of the biometric technology, a gradual approach for the development of the VIS biometric solution is recommended. A measure for keeping the accuracy to the appropriate level would be to increase the number of fingers used for matching or to reduce the database size by lowering the data retention period or filtering. In the VIS context, knowing that the database will start off quite small, the matching could, in the beginning, be performed with only a few fingers. The biometric solution should develop proportionally according to the VIS database volumes (from zero to 70 million records after five-eight years).

As a last resort visual checks using the VIS photographs can be performed in combination with biometric identification.

The preference for the use of flat instead of rolled fingers is the following:

1. Flat prints are **easier** and **faster** to take and no physical contact is necessary between the applicant and the official;

2. Flat prints are **less distorted** than rolled ones since in the latter case, fingers are quite often pressed too hard during the enrolment process;

3. Another important advantage lies in the fact that it will be perceived as **less intrusive**;

4. Due to the flat fingers stored in the database latent searches might, in some cases, not be successful. This slight drawback has to be put in relation with the advantages mentioned previously.

Investment costs on biometrics would be spread over several years. This will be discussed in further detail in chapter 7, which deals with investment and resource planning.

3.4 CONCLUSION

Using biometrics as an additional identifier would certainly support the VIS business processes. Considering that the architecture of such a system would be rather complex due to the high number of parties involved, the implementation would only be possible on a step by step basis.

In the meantime, large-scale biometrics databases will be more widely used than today, allowing for greater comparison, and so-called multi-model biometric systems will be available. For the time being, the only reliable technique is that of fingerprint. In addition, it is the only technique which supports the combat of terrorism or other kind of crimes. Even if the biometric technology changes, fingerprint databases will still be used for the next decades. This is not only true for Europe but also for the rest of the world. Furthermore, only a few biometric identifiers are suitable for comparing crime scene marks. Technical standards for fingerprint and photograph exchange are already defined and should thus speed up the implementation process. Finally, fingerprint comparison is becoming cheaper and cheaper and the matching algorithms are being further improved. This will result in higher speeds and accuracy.

This approach gives the most flexibility in terms of scaling, investment and tuning of accuracy depending on needs and experiences. If due to the size of the biometric database, accuracy declines (this situation could arise for instance in 5-7 years), a secondary biometric identifier could be implemented, such as facial recognition, so to bring the accuracy back to the appropriate level.

Any other future biometric features could be added if appropriate, i.e. features resulting in complementary information and improving the VIS processes.

However, the implementation of different biometric identifiers in different information systems will hinder identification in other systems. This might be intended, e.g. when it comes to privacy issues, but may also lead to undesirable situations when, for instance, visas are issued to wanted individuals or persons who are registered to be refused at border entry.

4. FUNCTIONAL, TECHNICAL AND OPERATIONAL REQUIREMENTS

A requirement is defined as a condition or capability to which the system must conform. Requirements management is the systematic approach to eliciting, organising, communicating, and managing the requirements of an information system, the VIS in this case. The input to the requirement management process is the comprehensive understanding of the actual user and **other stakeholders' needs that are to be fulfilled by the VIS**.

In the context of this study, the requirements specification process determines a set of high level and commonly agreed requirements that VIS will have to comply with. The possible solutions for the architecture of the VIS, which are introduced in Chapter 5, are designed to fulfil all these requirements.

With regards to the above, this chapter determines the VIS requirements at *functional*, *technical* and *operational* level.

4.1 FUNCTIONAL REQUIREMENTS

The functional requirements prescribe the actions the VIS must be able to perform. It starts with the definition of the data to be stored and processed by the system and subsequently derives the functionalities provided by the system.

4.1.1 Data requirements

VIS should store the following data:

1. **Alphanumeric data** pertaining to applicants, the uniform visa application form and the visa sticker. It should include:

   (a) The type of visas:
   - Visas requested;
   - Visas formally refused;
   - Visas issued, indicating type (A, B, C, D, D+C, LTV);
   - Visas annulled, indicating type;
   - Visas revoked, indicating type;
   - Visas extended, indicating type.

   (b) The study should assess the impact of including standard grounds for refusing, cancelling, withdrawing and extending visas;

   (c) All the data required to identify the applicant taken from the visa application form[8];

[8] Annex 16 of the Common Consular Instructions (OJ C 313 of 16.12.2002, p. 1[93]).

(d) All the data required to identify the visa derived from the uniform visa sticker[9]. This includes the unique visa number, the competent authority that issued it and whether the latter issued it on behalf of another state.

A complete record of alphanumeric data would require about 6 kB of storage space.

2. **Personal traits** pertaining to applicants:

(a) **Digitised photographs**. A digitised colour photograph compliant to the ICAO standard and compressed would require about 45 kB of storage space;

(b) **Biometrics** require storage of the samples (the image of the biometric identifier) and the templates (the extracted features of the biometric identifier). Depending on the biometric trait, the storage space needed varies:

* Fingerprint[10] (one finger):
  - Image: 25 kB;
  - Template: 0.25 kB.
* Iris (one iris):
  - Image: 2 kB;
  - Template: 0.5 kB.
* Face:
  - Image: see photograph;
  - Template: 1.3 kB.

3. **Supplementary (scanned) documents** pertaining to the visa applications. This could include:

(a) Travel documents;

(b) Persons issuing invitations;

(c) Those liable to pay board and lodging costs;

(d) Insurance policies :

(e) Other documents of a total size equivalent to six (6) A4 pages, or its equivalent of twelve (12) A5 pages or twenty-four (24) A6 pages.

When using an appropriate compression algorithm for scanned documents (JBIG2) the storage space needed for the complete set of documents is about 180 kB.

Alphanumeric data should be encoded using the Unicode Standard, which was designed to support the world wide interchange, processing, and display of written texts in most of the written languages currently in use in the modern world.

[9] Annex 8 of the Common Consular Instructions (OJ C 313 of 16.12.2002, p. 1[58]).
[10] The reported figure accounts for a single finger. A simple multiplication will introduce the storage requirements for a number of fingers.

4.1.2 Functions

The system would support four groups of functions:

1. Insert, update and delete data captured during the visa-issue process. Typical examples are:

   - Registration of a new visa applications in the system (insert function);
   - Update of an existing visa application (update function);
   - Delete of an existing visa application from the system after the 5-year expiration period (delete function).

2. Search, verify and retrieve data. Typical examples are:

   - Search for a person's identity based on biometric data (search function);
   - General search on alphanumeric data such as visa registration number, passport number, applicant name, or other personal particulars;
   - Verify the authenticity of a visa sticker (verification function);
   - Retrieve the visa information history of an applicant (retrieval function).

3. The VISION and SIS II consultation as determined in the Common Consular Instructions on visas for the diplomatic missions and consular posts.

4. Production of statistics as part of an automated reporting and statistics service. Indicative reporting requirements include:

   - Statistics per Country on the visas issued, refused, revoked, extended, or annulled;
   - Comparison charts per country;
   - Totals for each type of visa status (issued, refused, revoked, extended, or annulled) for applicants from a given country of origin;
   - Global totals by geographic region and (even) by consulate.

   Depending on the category of data, different types of searches should be supported by the system, including:

- For alphanumeric data: phonetic and trunk searches, including transliteration;
- For Biometric data: search types specific to each type of biometrics employed;
- For Supplementary documents: document search facilities will not include full textual search. Metadata based search facilities (e.g. metadata concerning the document) will be provided.

4.2 TECHNICAL REQUIREMENTS

In order to deliver the desired quality to the VIS end-user, the system must also exhibit a range of specifications that are not described by the system functional requirements. These are primarily quality attributes and for the sake of simplicity are referred to as **non-functional or technical requirements**.

Regarding such categories/types of requirements, the current section describes "technical" requirements pertaining to the *interfacing of the new system*, the *biometrics*, the *storage,* the *communications* and finally the *testing.*

4.2.1 Interface requirements

An explicit requirement is to investigate the following two types of interfaces:

1. A *system-to-system* interface:
   - Internal VIS system: C-VIS to N-VIS and N-VIS to other N-VIS;
   - External VIS system: Other systems (e.g. SIS or existing National Visa systems) to VIS and VIS to other systems. VIS will comply with a service-oriented architecture.

2. A *user-to-system* interface: end-users to N-VIS. The interface should accommodate two types of connectivity:
   - A connectivity that allows quick transfers between the end user premises and the VIS;
   - A connectivity that tolerates longer delays between requests and answers.

The VIS system should be based on a service-oriented architecture that offers open standard interfaces and messages (XML) for interfacing with other systems.

4.2.2 Biometric requirements

It should be possible for the users of the VIS architecture to use biometric capturing devices from different vendors. In order to achieve this, since biometric templates are always proprietary **only the images (the scanned image of the biometric identifier) can be sent to the central biometric system for features extraction (creation of the template) and matching**. For the sake of interoperability the format of the samples should be an open standard (like JPEG for instance). For accuracy reasons the samples should be captured with a minimal resolution.

It must be possible to obtain a biometric trait from minimal 97% of the persons.

Accuracy is a key requirement for biometrics and minimum requirements are the following:

- For verification:
  - Accuracy > 99.9%.

- For identification (taking account of 70,000,000 enrolees):
  - Accuracy > 99.0 %.

4.2.2.1 Enrolment station requirements

For safety reasons, there should be no physical contact between the applicant and the officials. As a result the following requirement apply to the biometrics scanner:

- Failure-to-enrol rate < 1%;
- If technology requires contact with equipment it must be easy to have the surface cleaned by an applicant (not by staff);
- Minimal personal assistance needed for enrolment;
- No physical contact needed between Applicant and official;
- 100 % non-hazardous;
- Perform a quality check during the acquisition procedure;
- Equipment must work under various climate conditions temperature –10°C 50°C and humidity 0% - 90%).

4.2.2.2 Operational requirements

- Maximum enrolment time 3 minutes;
- Time between enrolment 2 minutes, including cleaning (if needed);
- Low maintenance, maximum one on-site servicing a year;
- The image (result of a scan) must be based on open standards;
- Maximum size of image without encryption 0.4 Mb.

4.2.3 Storage requirements

The data volume requirements for the various categories of data mentioned in section 4.1.1 have been estimated on the basis of 20 million visa requests per year over a five-year period of retention. These requirements can be summarised as follows:

1. Alphanumeric data and indexes require 600 and 12 Giga-bytes of storage respectively;
2. Photographs require 3.2 Tera-bytes of storage;
3. Supporting document data require 18 Tera-bytes of storage;
4. Biometric samples and templates have different storage requirements depending on the biometric trait. In case of fingerprints with ten-print images, VIS will require 17 Tera-bytes of storage.

The aggregate amount of storage space will be distributed over the various locations of the VIS. Since the VIS database will be progressively, gradually loaded, the storage requirements will likely evolve as shown in Figure 7-1.

4.2.4 Communication requirements

Two types of networks are to be considered:

1. The network that interconnects the C-VIS and the various N-VIS; This is known as the Trans-National Domain;

2. Networks that interconnect each N-VIS with their national users; These are known as the National Domains.

The explicit requirement of the study is to assess the use of the SISNET and TESTA II communication networks to act as the Trans-National Domain. The network should provide security, latency, bandwidth and availability as defined by the security (section 4.3.1), response time (section 4.3.1.2) and availability requirements (section 4.3.1.1) of the system.

There are no specific requirements for the National Domains.

4.2.5 Testing environment

A separate *development and testing* environment would have to be foreseen as an integral part of the VIS. It will enable validation and acceptance of the various VIS components. It shall be used for:

- testing and debugging new application releases (known as beta testing) and application components;

- running data migration tests to ensure data and application integration;

- testing of the various systems and sub-systems (e.g. biometric engines, database components);

- testing of the entire system (once all the components have been accepted) to ensure that when all components are integrated they yield the expected result.

4.3 OPERATIONAL REQUIREMENTS

In order to deliver the desired level of service to the VIS end-users and stakeholders, the system must exhibit a range of characteristics that could be described primarily as quality attributes. These are referred to for simplicity as **operational requirements** concerning *reliability, security* as well as *technical support* of the implemented solution.

4.3.1 Reliability

4.3.1.1 Availability requirements

VIS should be operational on a round-the-clock basis (24 hours a day, 7 days a week), and should shield the users from any unscheduled or otherwise unacceptable disruption of service. Table 4-1 shows the maximum permissible downtimes for the various business processes supported by the system.

Table 4-1: Availability for the various business processes.

Business process	Service hours (GMT)	Max. monthly down-time	Min. mean time between failures	Max. mean time for repair
New visa without previous registration	24 h/24 h 7d/7d	2 h (99.7%)	48 h	1 h
New visa with a previous registration	24 h/24 h 7d/7d	2 h (99.7%)	48 h	1 h
Person identification	24 h/24 h 7d/7d	2 h (99.7%)	24 h	1 h
Visa and traveller verification	24 h/24 h 7d/7d	1 h (99.9%)	48 h	5 min.

The monthly down-time refers to the total amount of time the system could be interrupted within a 30-day period. The mean time between failures refers to the minimum time that should pass between two consecutive service interruptions. The mean time for repair refers to the time necessary to restart the service.

Considering the high level of availability required, hardware-level redundancy should be employed in order to avoid single points of failure in the VIS sub-systems. Such redundancy would provide business-process continuity with little or no possibility of serious or significant service interruption. In rare cases where problems do occur, response times might increase slightly during the time needed to effect repairs.

4.3.1.2 Contingency requirements

Business continuity requirements aim to ensure that essential functions and operations can continue when the production system is seriously damaged or even destroyed. VIS should support business continuity in the event of failure of the production system. Thus, fallback systems have to be established for the Central (C-VIS) as well as for each of the National Visa Information Systems (N-VIS) in different locations.

VIS should be designed to meet a “zero data loss” business continuity strategy with immediate and automatic transfer to the business continuity system. Local and remote copies of all the data should be fully synchronised, with full network switching capability between the production and the business continuity systems. The length of time required to switchover between the two systems should be less than 5 minutes.

From a technical perspective the “zero data loss” strategy requires setting up business continuity systems with hardware, data storage, software and communications capabilities similar (or in some cases identical) to those of the production site. This configuration **is that which has been used in designing and pricing the technical solution for the VIS**.

With regard to the *management* of the business continuity, the following requirements should be met:

1. Provision for contingency planning at the central (C-VIS) and national (N-VIS) levels;

2. Contingency planning co-ordination;

3. Contingency plan testing to confirm the validity of individual recovery procedures and the overall effectiveness of the plan;

4. Training for personnel exercising contingency plan responsibilities;

5. Location of the BCS (Business Continuity System) at least 50 km from the production site;

6. Location of the maintenance staff at least 100 km from the production site.

4.3.1.3 Performance requirements

The response-time[11] requirements for the supported processes are illustrated in Table 4-2 for two different scenarios. The figures given refer to the time elapsed between the submission of a request and the reception of an answer or reply.

For further information concerning the business processes, refer to chapter 2 herein, or to Annex B, which details the VIS business processes.

Table 4-2: Response-time requirements (end user perspective).

Business process	Scenario T1 (normal)	Scenario T2 (fast)
New visa without previous registration	4 h	30 m
New visa with a previous registration	2 h	15 m
Person Identification	4 h	30 m
Visa and traveller authentication	20 sec	5 sec

Table 4-3 shows the corresponding times spent in the VIS system, i.e. the time necessary to process the request and to traverse the network.

Table 4-3: Response-time requirements (N-VIS to C-VIS).

Business process	Scenario T1 (normal)	Scenario T2 (fast)
New visa without previous registration	2 h	15 m
New visa with a previous registration	1 h	8 m
Person Identification	2 h	15 m
Visa and traveller authentication	10 sec	3 sec

4.3.2 Security requirements

The five primary functions of a good security framework include[12]:

1. **Authentication**: to verify with confidence the identities of the users;

2. **Access control**: to enable only authorised users to access appropriate resources.

3. **Privacy**: to ensure confidentiality of communication among authorised parties and of data in the system;

4. **Data integrity**: to ensure that communications, files and programs are not tampered with;

[11] Response time accounts processing delay and network latency. It does not account the time necessary to conduct the administrative procedures.
[12] In Information Security Management Handbook, 4th Edition, Tipton & Krause, Auerbach, p433

5. **Non-repudiation**: to provide undeniable proof that a certain user sent a certain message and to prevent the receiver from claiming that a different message was received.

The Technical Annex defines the scope of the analysis of the VIS security:

- An information classification for the VIS data should be elaborated in order to ensure the level of confidentiality appropriate to the sensitivity of the data moved and stored inside the VIS system;

- All the necessary measures and controls to ensure the invulnerability of the VIS should be foreseen (prevention, detection and correction). This includes encryption, user authentication, physical protection, monitoring, reporting and auditing.

The Technical Annex also introduces a few organisational requirements the security solution should satisfy:

- Data ownership. As mentioned in the Council Decision (2001/264/EC), all information stored or processed by the VIS system should have an owner, responsible for the proper use of and access to the data. In the context of the EU, and in order to remain consistent with the existing business processes, the ownership of a record should remain at the national level delivering the corresponding visa, i.e., with the consulates. This however is subject to the existence of a supporting legal framework, which does not yet exist. This implies that data CANNOT be updated by a consulate other than that which has "proceeded to enrolment";

- Two types of access are foreseen and should be restricted to the corresponding categories of users:
  - Insertion and updates of data is restricted to people involved in the visa issuing process;
  - Consultation of data is restricted to the previous category and also to:
    - Officials involved in the control of borders;
    - Police departments;
    - Immigration departments;
    - Possible other authorities.

- Access of the users has to be provided and controlled by the corresponding Member State;

- Member States are responsible for operating the equipment located at users' premises and managing local operations;

- Member States are free to operate national visa systems and to inter-operate them with the VIS system.

The following answers the information classification as well as the measures and controls for ensuring the invulnerability of the VIS.

4.3.2.1 Information and assets classification

Regarding the Council Decision 2001/264/EC, section II, which concerns classifications and markings, VIS information qualifies for the classification level "UNCLASSIFIED" or as 'EU RESTRICTED". The 'EU RESTRICTED" classification level is applicable to information and

material the unauthorised disclosure of which *"could be disadvantageous to the essential interests of the European Union or of one or more of its Member States"*.

The impact of the different classification levels is described in the table below.

	Unclassified	EU-Restricted
Information	No security.	Can be handled in standard administrative environment with additional organisational and technical measures: ▪ Need to know (restricted access); ▪ Physical protection. ▪ Destruction procedures. ▪ Personnel awareness. ▪ Protection should extend to all concerned media (paper, IT equipment etc).
Information Systems	No security.	The security standard requirements are complemented with additional specific security products and rules such as: ▪ Physical security measures. ▪ Enhanced workstation and server security. ▪ Specific logging, auditing, alerting rules. ▪ Encrypted transmission and storage.

The above should be consulted when determining the appropriate protection level for information and processing systems.

At the present time, no classification for the information and assets has been made. However, the classification of "EU-restricted" is assumed for the purposes of the present study.

	EU-Restricted
Alphanumeric data (visa application and visa sticker) and supplementary documents	X
Biometric data and photographs	X
VIS assets (hardware and software)	X

4.3.2.2 Measures and controls requirements

4.3.2.2.1 Authentication[13]

Authentication of a claimed identity can be established in four ways:

- What you know (passwords and pass phrases);
- What you have (tokens: physical keys, smart cards);
- What you are (static biometrics: fingerprint, face, retina and iris recognition);
- What you do (dynamic biometrics: voice, handwriting and typing recognition).

The authentication mechanisms should be based on a combination of two methods: what you know (a password) and what you have (a token generated by a one-time password generator).

4.3.2.2.2 Access control[14]

Access control (or authorisation), as the name implies, deals with ensuring that users only have access to appropriate resources (systems, directories, databases and records) as determined by the security policy administrator. Technologies commonly used to enforce access control include trusted operating systems through the use of access control lists (ACLs), single sign-on products and firewalls. Single sign-on products enable a user to authenticate to the environment once per session. The user will thus be authorised to access any of the appropriate resources without the need for additional authentication during that session.

4.3.2.2.3 Privacy

Depending on its sensitivity, information must be rendered indecipherable to unauthorised people, whether stored on disk or communicated over a network. The recommended solution is to implement a cryptographic environment enabling users to maintain and exchange encrypted information using PKI keys.

4.3.2.2.4 Data Integrity

Integrity involves the protection of data from corruption, destruction or unauthorised changes. This requirement also extends to the configurations and basic integrity of services, applications, and networks, which must be protected. Maintaining the integrity of information is critical. When information is communicated between two parties, the parties must have confidence that it has not been tampered with. Conceptually similar to checksum information, most cryptographic systems provide an efficient means to ensuring integrity. The recommended solution is an electronic signature system based on PKI certificates.

4.3.2.2.5 Non-repudiation

It is necessary to ensure that electronic transactions provide some form of proof of sender and message received when they are completed. This requirement goes with the need to verify

[13] In Computer Security Handbook, 4th Edition, Bosworth & Kabay, Wiley
[14] In Information Security Management Handbook, 4th Edition, Tipton & Krause, Auerbach

identity and control access. The recommended solution is the same as above: an electronic signature system based on PKI certificates.

4.3.3 Technical support requirements

The VIS organisations will have to provide resources to apply preventive measures including implementation of rigorous systems maintenance procedures, continuous system monitoring and the implementation of the procedures laid down in the business continuity plans.

In a view of this, an explicit requirement is to set-up **technical support units (TSU)** at the central (C-VIS) and national levels (N-VIS). These units would be in charge of managing the VIS components to prevent interruption of VIS services (insure business continuity), and in case of difficulties, of re-establishing full functioning as swiftly and as smoothly as possible.

The TSU is defined as a unit (composed of a team of experts) in charge of running the VIS maintenance and operations. The unit should provide management services, information facilitation, and help-desk services for the VIS.

4.3.3.1 Maintenance and management requirements

Maintenance procedures should ensure the availability and performance of the VIS system (C-VIS + N-VISes). Maintenance encompasses the following:

- Change in the data model;
- Update or upgrade of existing applications;
- Changes to the system hardware configuration;
- Changes to the networking environment;
- System repair.

Management procedures should ensure the following:

- Co-ordination of maintenance;
- Application of the security policy (including management of access lists);
- System monitoring and reporting;
- Testing of new hardware and software;
- Contingency planning.

Maintenance and management tasks for the VIS will be undertaken by the Technical Support Units (TSU) located at the C-VIS and N-VIS sites under the responsibility of the organisations in charge of the VIS operation.

Member States will also need to set up Technical Support Units in order to provide the necessary technical support to the world-wide diplomatic missions, consular posts or other national users using the VIS. This technical support encompasses the installation and maintenance tasks dedicated to consulates equipment or other equipment related to the VIS.

The central Technical Support Units will also keep the national Technical Support Units informed of any change in the VIS system and provide the required technical training. Accordingly, co-ordination between central TSUs and national TSUs should be foreseen.

4.3.3.2 Back-up and archiving requirements

As a fallback system will exist in parallel, and be continuously updated, the back-up operations could be planned at this fall-back site in order not to disturb the production site.

The following archiving and back up policy would be considered as a requirement during the design of the systems:

- Periodic backup of all information; weekly, for instance;
- Immediate backup of new information;
- Archiving of data after the retention period (five years) should be considered.

4.3.3.3 Help-desk support requirements

An explicit requirement is to have a Help Desk and Assistance centre operated at both the central (C-VIS) and the national levels (N-VIS).

The former should provide technical assistance services to the national systems (N-VIS) the goal being to maintain the highest possible business continuity of the VIS.

The latter will provide support diplomatic missions and consular posts and other national authorities with access to the VIS.

The Help desk should be manned with experts trained to support the VIS systems and in the operating procedures performed by the visa issuing offices.

Help Desk personnel would:

1. Answer direct calls from consular officers in order to provide technical assistance regarding problems they encounter with the VIS standard configuration;
2. (optionally) Maintain the database of all requests, including actions taken to resolve the problems, identity of originating parties, etc…

The help-desk should operate on a round-the-clock basis (24 hours a day, 7 days a week).

4.3.4 Segmentation requirements (N-VIS and consular posts)

The size of an N-VIS will depend on the number of visa requests handled by the corresponding Member State. As the number of visa requests varies widely from Member State to Member State (see Table 4-4), one size will not fit all. The same principle applies to the consulates, which exhibit even larger variations in the number of requests handled (between 200 up and 100,000+ yearly).

Table 4-4: Visa statistics for visa requests among Schengen Members.

MS	Visa requests
Germany	3 200 000
France	2 600 000
UK	1 700 000
Italy	1 200 000
Spain	800 000
Greece	630 000
Austria	540 000
Finland	480 000
Netherlands	420 000
Belgium	200 000
Sweden	200 000
Portugal	155 000
Denmark	120 000
Norway	120 000
Ireland	68 000
Luxembourg	20 000
Iceland	15 000

Accordingly, a segmentation method has been applied at the N-VIS and consular post levels, which is based on visa statistics provided by the EC. The segmentation led to three N-VIS standard configurations that cover the range of N-VIS's (Table 4-5) and to three consulate standard configurations that cover the range of the consulates (Table 4-6).

The standard configurations will be sized and the corresponding costs will be reported in the study. Then each Member State will be able to derive sizing and costs proper to its particular situation by simply interpolating between the figures pertaining to the standard configurations.

Table 4-5: Segmentation of N-VISes.

	Category I (small)	Category II (medium)	Category III (large)
# yearly visa requests	100,000	500,000	2,500,000

Table 4-6: Segmentation of the local systems for the consulates.

	Category I (small)	Category II (medium)	Category III (large)
# yearly visa requests	500	5,000	50,000

4.4 STANDARDS

A common requirement is to provide solutions that are based on open standards as much as possible.

1. Security standards include:
   - The Council Decision 2001/264/EC[15];
   - The Decision of the Commission 2001/844/EC[16];

[15] OJ L 101, of 11.4.2001, p.1
[16] OJ L 317, of 3.12.2001

- The Strategic document of the Commission's security service "Information Systems Security Architecture" (http//europa.eu.int/comm/di/pubs/secty/secty_fr.pdf).

2. The applicable standards for *ICT coherence* and *interoperability:*
   - the Informatics Architecture (Release 8 – August 2001);
   - the IDA Architecture Guidelines at the Commission (http//europa.eu.int/comm/di/pubs/arch/architecture8_en.pdf).

3. Regarding the uniform format for visas: For the photograph, the minimum acceptable resolutions are 300 ppi (Pixel per inch) for scanning, and 720dpi (dot per inch) for printing. The size of the photograph must conform to the ICAO standard (26x32mm), whereby the head size from chin to crown must be between 70 and 80 percent of the vertical dimension of the portrait area;

4. The ICAO-recommendations (Document 9303) for alphanumeric data and machine readable documents;

5. The ANSI-NIST file format used for fingerprints and photographs;

6. Full support for all European languages. To this end, the 16-bit implementation of the Unicode standard (UTF-8) provides a simple and interoperable encoding scheme for all European character sets. Application components and the database should support this 16-bit encoding;

7. The XML standard (refer to www.w3.org) could also be considered as it includes Unicode specifications for message exchange;

8. The specifications for the visa sticker as given in Annex 8 of the Common Consular Instructions on visas for the diplomatic missions and consular posts (OJ C 313 of 16.12.2002, p. 1[58]);

9. The uniform visa application form for Schengen visas, as introduced in Annex 16 of the Common Consular Instructions on visas for the diplomatic missions and consular posts (OJ C 313 of 16.12.2002, p. 1[93]).