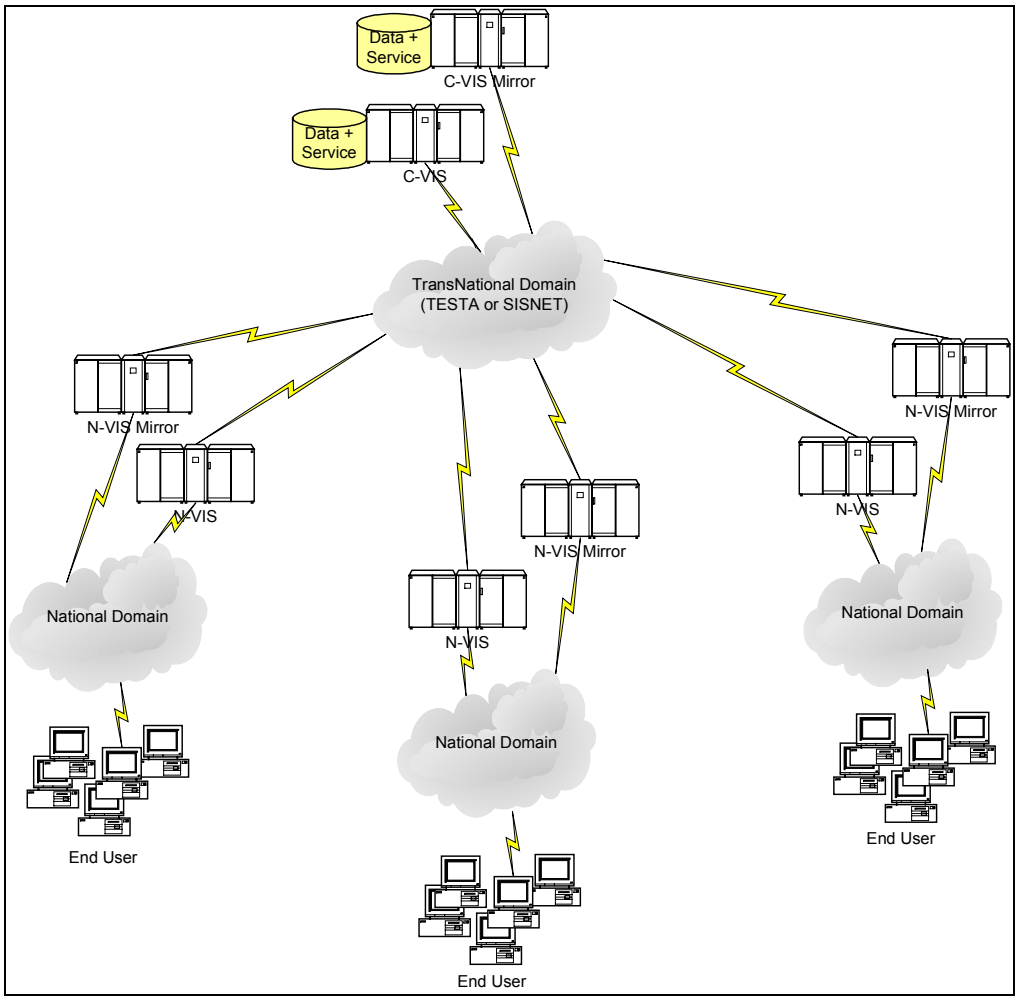
Table 9-16: Software configuration: test system.

Software	Configuration	Units	Unit price (€)	Total price (€)
Application Server (1)	Application Server Enterprise	2	21,720	43,440
	ONE Messaging Server (only 100 mailboxes)	100	22	2,200
	ONE Web Server	1	1,650	1,650
	ONE Message Queue	2	4,000	8,000
Database Management System (2)	Server Enterprise Edition	2	43,440	86,880
	Management Packs	2	9,774	19,548
	Advanced Security	2	10,860	21,720
	Label Security	2	10,860	21,720
Identity Manager (3)	ONE Directory Server	100	2	200
Backup/Archive manager (3)	Solstice Backup	1	21,400	21,400
System Management (5)	Management Center 3.0 Advanced Systems Monitoring	1	3,250	3,250
Biometric matching iris (7)	Know-who	1,000	1.0	1,000
Biometric matching iris (7)	SQL server single user license	1	650	650
Biometric matching face (7)	FaceExplorer	1,000	0.5	500
Biometric matching face (7)	Server Enterprise Edition	1	43,440	43,440

9.3 CONFIGURATION FOR THE BUSINESS CONTINUITY SYSTEM

Business continuity could be assured by mirroring the C-VIS and each N-VIS in a different location (Figure 9-6). **Each mirror site should host a configuration identical to the original site**. The databases should be synchronised via specific software provided by database management system vendors. The business continuity policy will allow switching in minutes to a back-up sub-system in case a failure occurs anywhere in the VIS architecture.

Figure 9-6: Configuration for the Business Continuity System.



9.4 STANDARD CONFIGURATION FOR CONSULATES

Figure 9-7 shows a logical view of the various components of a consulate issuing visas. The hardware and software configuration chosen to implement consular components is described in Table 9-17 for category III, in Table 9-18 for category II and in Table 9-19 for category I. Numbers that appear between parenthesis refer to the specific machines on which the software will run.

Figure 9-7: Configuration at visa issuing offices.

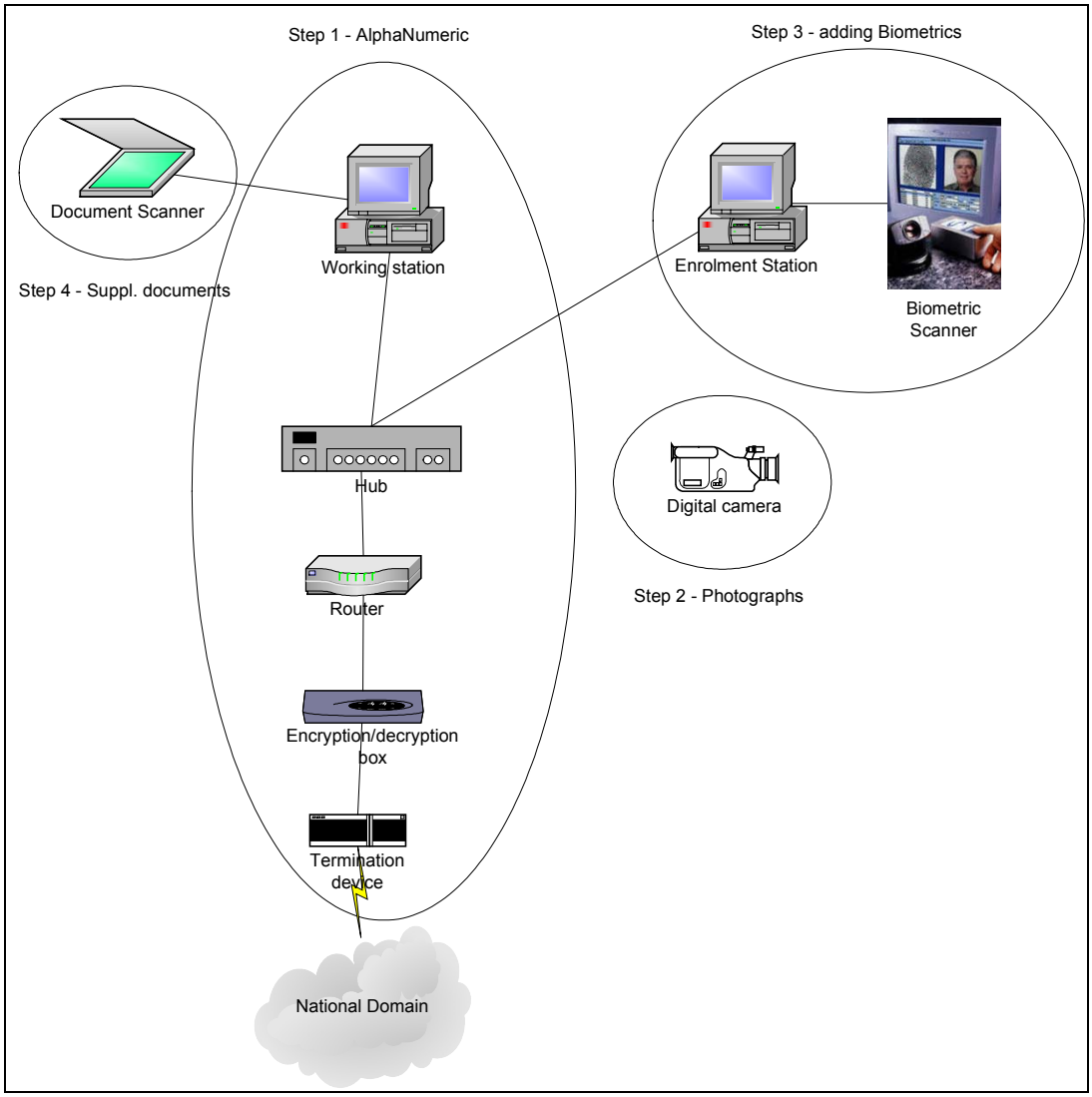


Table 9-17: Hardware and software configuration – consulates III.

Hardware	*Configuration*	*Units*	*Unit price (€)*	*Total price (€)*
Working station		9	1 500	13 500
Document scanner	i60	9	3 000	27 000
Digital camera		9	1 000	9 000
Biometric enrolment station	PC connected to a biometric scanner	2	10 000	20 000
Hub		1	150	150
Router	1721	1	900	900
Crypto box management PC		1	1 500	1 500
Software	*Configuration*	*Units*	*Unit price (€)*	*Total price (€)*
E-mail client (1)	Eudora (price based on 1 user licence)	9	40	360
Imaging	Include with Scanner	9	0	0

Table 9-18: Hardware and software configuration – consulates II.

Hardware	*Configuration*	*Units*	*Unit price (€)*	*Total price (€)*
Working station		1	1 500	1 500
Document scanner	i60	1	3 000	3 000
Digital camera		1	1 000	1 000
Biometric enrolment station	PC connected to a biometric scanner	1	10 000	10 000
Hub		1	150	150
Router	1721	1	900	900
Crypto box management PC		1	1 500	1 500
Software	*Configuration*	*Units*	*Unit price (€)*	*Total price (€)*
E-mail client (1)	Eudora (price based on 1 user licence)	1	40	40
Imaging	Include with Scanner	1	0	0

Table 9-19: Hardware and software configuration – consulates I.

Hardware	*Configuration*	*Units*	*Unit price (€)*	*Total price (€)*
Working station		1	1 500	1 500
Document scanner	i60	1	3 000	3 000
Digital camera		1	1 000	1 000
Biometric enrolment station	PC connected to a biometric scanner	1	10 000	10 000
Hub		1	150	150
Router	1721	1	900	900
Crypto box management PC		1	1 500	1 500
Software	*Configuration*	*Units*	*Unit price (€)*	*Total price (€)*
E-mail client (1)	Eudora (price based on 1 user licence)	1	40	40
Imaging	Include with Scanner	1	0	0

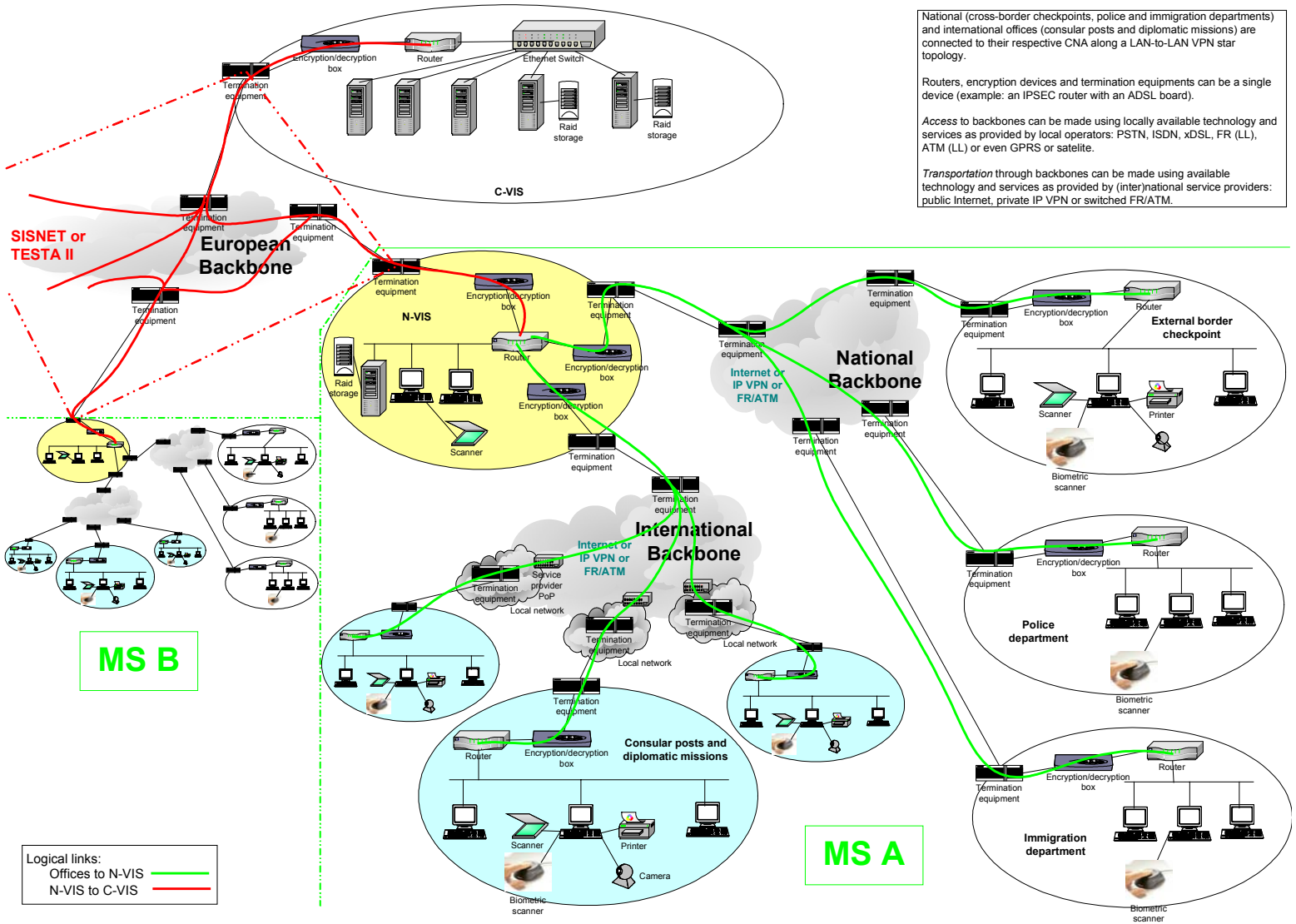


Figure 9-8: Global System Architecture for the VIS

10. CONCLUSIONS AND RECOMMENDATIONS

This section reviews the major issues following the Council Guidelines.

10.1 BASIC ARCHITECTURES

Under the precondition that VIS must have a similar architecture to that of the existing Schengen Information System, two fundamental architectural options have been considered:

- a separate VIS (option 1), or
- a technical integration of VIS and SIS II, in view of the synergies (option 2).

Option 1: Separate VIS system

There are only two variations on this solution, suitable for this purpose (**centralised** or **hybrid**). Both solutions equally support the VIS business context.

1. In the **centralised solution**, all the data and functions are exclusively located at the central level (C-VIS);
2. In the **hybrid solution** only basic data (mainly alphanumeric data and indexes) is stored at the central level (C-VIS), while bulk data (such as photographs, biometric images, scanned documents, etc.) are stored at the corresponding national level (N-VIS).

Option 2: Technical integration of the VIS and SIS II

The two feasible solutions exhibiting the synergistic architecture are:

1. Solution 1, employs a **common technical platform**, has both systems located in the same building, connects them to the same network through a single access point, uses the same technological platforms and allows for the sharing of management tools and staff between the two systems;
2. Solution 2, utilising a **common technical platform and services**, introduces synergies at the application level in addition to those commonalties described above (pt.1). The systems share or use common services as well as the biometric components.

For Option 1, using the separate VIS, it is recommended to opt for a centralised solution. The solution introduces operational efficiency, is less expensive and entails less in the way of systems administration. It provides a moderate risk profile making it a clear favourite.

For Option 2, the technical integration of VIS and SIS II at central level is recommended, as it significantly reduces the overall investment and associated operational costs of the two systems. In order to maximise the synergies between the two systems, it is suggested to implement VIS and SIS II in parallel, possibly even launching a common call for tender covering the construction of both systems. Likewise, it is advisable that the project management concerning the implementation be assumed by a single organisation.

All things considered, it is recommended to opt for Option 2 / Solution 1: sharing a common technical platform between VIS and SIS II. Technology convergence will

introduce cost savings. Moreover VIS and SIS could share common maintenance and administration procedures and thus technical human resources supporting these operations.

The solution of the common technical platform and services (Option 2 / Solution 2), despite its advantages, may introduce additional complexity to the application development. Nevertheless, it should be considered carefully if only for the additional and significant cost savings which could be expected.

10.2 VISA INFORMATION TO BE STORED AND PROCESSED

VIS should be engineered and appropriately sized for the ability to store large amounts of alphanumeric data, digitised photographs, biometric information and scanned documents supporting the visa application. In quantitative terms, the VIS should be designed to process 20 million visa requests per year. This is expected to cover the needs of the Member States and accession countries, as well as of Iceland and Norway, for the next five years.

Over a five (5) year retention period, the number of visa applications stored in the VIS will reach the 100 million mark. 70 million of these applications will include specific information (photographs and biometrics) mainly due to multiple applications by frequent travellers. The total volume requirements are estimated as follows:

- for alphanumeric data : 0.6 TeraBytes[27];
- for photographs : 3.2 TeraBytes;
- for fingerprints (based on total of ten fingers) : 17 TeraBytes;
- for supporting documents: 18 TeraBytes.

Such volumes can be handled adequately by the technology currently available.

It is recommended that a phased approach be followed in the establishment of the VIS, beginning with a scaled-down system, followed by upgrades, based on the evolution of volume and transactional capacity requirements. In particular, it is recommended to start with a nominal system configuration capable of handling 20% of the total volume and transaction capacity. Once storage and processing capacity reaches the 80% usage level, an upgrade should be initiated (this situation could arise for instance in 3-5 years, as more world-wide consular posts connect to the VIS). This approach affords the most flexibility in terms of scaling investment according to the roll-out of the consular posts.

10.3 BIOMETRICS

Whereas the sharing of alphanumeric data improves the existing procedures of visa issuance and control, it fails to uniquely identify persons or to verify claimed identities. Just consider the number of persons that share "Smith" as a common name and the difficulties in uniquely identifying these persons in an efficient way.

[27] 10^{12} bytes.

The precondition towards objective internal security and combating terrorism makes the use of biometrics imperative. Biometrics will assist in determining a unique and fixed identify for a person (travellers or other aliens).

In the VIS context, biometrics will be used to support the verification and identification procedures during visa issue and during the control procedures at cross-border and other checkpoints. It is the unique means to accurately identify a person, to determine if an applicant has previously applied for a visa under a different identity as well as to determine whether the applicant has background records.

Fingerprint, Iris and facial recognition are possible candidates for the purposes of the VIS. Fingerprints should be used as the primary biometric identifier in both modes, i.e. identification and verification. Facial recognition could be considered, but only under the precondition that photographs be captured in a uniform way complying with certain common standards, which would make them suitable for computerised facial recognition in the future.

One should not invest in iris or another biometric technology as long as the new technology in question has not been proven. Given the number of embassies, consulates and entry/exit points potentially involved, the risks associated with such a significant investment, in both monetary terms and resources, would be very high. Iris recognition might be developed further later on, once market maturity has reached a reasonable level.

In its current state, the SIS will only store biometrics. In view of this significant development, both systems should share a common biometric technology. This will introduce synergies at operational and technical levels and will create significant cost savings that will have an impact on the total cost of ownership of the VIS and SIS.

It is therefore recommended that fingerprints be used as the primary biometric identifier in both modes, i.e. for identification and verification. It is currently the only fully reliable biometric technique, proven via large-scale implementations, that supports combating terrorism or other categories of criminal activity and provides for interoperability with existing fingerprint databases operated by the Member States. Even if the biometric technology changes, fingerprint databases will still be in use over the next several decades. Fingerprint technology is becoming cheaper and matching algorithms are being continually improved. This will result in higher speed and accuracy. This approach gives the most flexibility in terms of scaling investment and tuning of accuracy depending on the needs and experiences. If, due to the size of the biometric database, accuracy degrades (this could be the situation for instance in 5-7 years), a secondary biometric identifier could be introduced (such as facial recognition) to bring the accuracy back to the appropriate level.

Fingerprints would facilitate background checks against latent data stored in national information systems.

In the SIS context, biometrics might be used in the future to uniquely identify persons for the purpose of refusing entry or in order to determine whether they pose any other security threat. In view of the SIS II, it is recommended that a shared common biometric solution be used for the VIS and SIS II. This will have significant benefits. At the end-user level a common biometric infrastructure will be required. This ensures the future interoperability between the VIS and SIS as VIS users could perform background checks in the SIS and vice versa. Moreover, the use of a common identifier will introduce openness to other systems operated by the Member States which use the same biometric identifier (fingerprints).

10.4 COMMUNICATION INFRASTRUCTURE C-VIS TO N-VIS

The existing networks, SISNET or TESTA do not meet the availability requirements for the critical process of visa and traveller verification. Thus these communication infrastructures need to be upgraded to support the VIS. In the SISNET case the current contractual arrangements expire in 2008 and cannot be extended. Similarly in the case of TESTA II the contract expires in 2005.

It is therefore recommended to opt for a complete new communication infrastructure. The total set-up time for a new infrastructure will be at least 18 months and will entail significant administrative burdens in addition to large investments.

From a strategic point of view, its is recommended to closely follow the developments of the network that will replace TESTA II (i.e. the future TESTA III network).

TESTA III would meet the technical requirements of the VIS and in particular the availability, quality of services and bandwidth capacity. In anticipation of this network, DG-JAI has taken some preliminary steps to ensure that the future TESTA III procurement contract has been drawn-up to meet the required availability requirements of the VIS and the SIS II.

10.5 COMMUNICATION INFRASTRUCTURE N-VIS TO CONSULATES

Secured world-wide networks with sufficient communication capacity (bandwidth) are required to connect each consular post to its respective 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 infrastructures.

Member States, which do not possess network infrastructures connecting their consular posts, will have to launch a process in order to establish provisions for such a network in anticipation of the VIS. Nevertheless, the communication requirements for connecting consular posts to the N-VIS are moderate and are, today, commonly available from international telecommunication operators.

As a precondition for the viability of VIS, Member States should take appropriate measures, in a timely manner, to establish new communication infrastructures or to upgrade their existing ones, if needed, between consulates and the N-VIS.

10.6 VISION NETWORK

From a purely technical perspective, the VISION consultation network relies on outdated technologies based on X.400 messaging exchanges. In light of this drawback, it is recommended to develop the VISION consultation network in the VIS as an integral part of the visa issuing process. This would marginally increase the VIS application development costs. However, the expected cost savings in system and application maintenance would offset those costs. The total cost savings is estimated at 1.2 Million Euros per year. More significantly, it will have a strong impact on the business processes from an end user perspective. VISION consultation will actually be embedded inside the VIS visa issuing business process and will be totally transparent for the end user.

In conclusion, the VISION consultation network should be developed as part of the standard VIS functionality.

10.7 VIS ROLL-OUT PLANNING

The VIS is a unique and technically feasible system for the exchange of visa data between the Member States. Overall, it is a complex and expensive system that will require large investments starting from 2003 to 2010 and beyond.

From a technical and operational perspective, it is recommended that the central system, the C-VIS, be developed in a single step (alphanumeric, photographs, biometric). The national components, the N-VIS, will be developed in a similar manner (single step approach). The strategic objectives of VIS can only be met once the first three data types (alphanumeric data, photographs and biometric identifier) have become part of the system.

Member States have the flexibility to adopt an incremental approach to the roll-out, providing their consular posts and other authorities with the hardware and communication infrastructure in the form of a standard configuration for offices issuing visas. Member States can start by sharing only alphanumeric data, later introduce photographs, then biometrics and finally supporting documents. The commitment of the Member States is the precondition to the development of the VIS. Data will have to be registered in the VIS from the Member States' consular posts world-wide. Only then can data be shared between the Member States.

Member States would have the flexibility to adopt an incremental implementation approach for connecting their consular posts to the VIS infrastructure. Regarding the central part (C-VIS) it is recommended that it be developed in a single step.

10.8 LOCATION FOR THE C-VIS AND N-VIS

In terms of physical hosting, 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 at least 10 Km from the primary C-VIS. In a similar manner, the N-VIS, one in each Member State, should be physically established in a major city possessing the necessary communication and security infrastructures as well as other technical facilities.

10.9 BUSINESS CONTINUITY

VIS will be developed with a primary focus to provide very high business continuity and thus availability. The business continuity policy assumes fully sized mirror sites, comprising exact replicas of the primary sites. The cost of a fully sized business continuity system for the C-VIS is almost as costly as the production site.

One alternative could be that the production and the business continuity systems are sized to 75% processing capacity each, with load balancing applied between these sites. This will have a significant impact on costs. However this approach introduces the risk of increasing response times in the event of failure of the production site, as the processing capacity to support the VIS operations would be limited to 75%.

10.10 INTEROPERABILITY WITH EXISTING NATIONAL SYSTEMS

The requirements for the development of the VIS have emphasised the need for open standards allowing an easy interoperability with existing systems like the Member States' current visa systems. Accordingly we recommend a service-to-service interoperability which is based on modern communication standards for web-services (HTTP) or messaging services (XML).

The development of the VIS will be based on open and commonly adopted standards that will facilitate integration, interoperability and data sharing with existing systems.

The VIS will have a service-oriented architecture that will support interoperability with other systems, which also capitalise on the open standards HTTP for application protocol and XML for message exchange.

10.11 DEVELOPMENT OF THE VISA STICKER

VIS will be engineered to support a critical business process of visa and traveller verification at border and other checkpoints. This requires a network availability of 99.9%, resulting in high networking costs.

Independently, VIS visa and traveller verification could be implemented off-line without the need to connect to the VIS. The visa and traveller verification procedures require storing a trusted copy of both the visa sticker information and a copy of the biometric identifier image of the visa holder. Today, it is possible to store such information in portable devices, e.g. contactless chips. Cross-border checkpoints equipped with specific terminals can read the information stored in portable devices for person verification. The integration of the contact-less chip in the visa sticker will require the necessary legislative procedures.

Contact-less chips in the visa sticker will facilitate the off-line visa and traveller verification, without connectivity to the VIS. This lowers telecommunication costs and has a small impact on the processing power requirements for the VIS infrastructure. However, the introduction of contact-less chip technology entails significant investments in specific hardware such as programming devices and readers.

10.12 THE ROLE OF THE TECHNICAL SUPPORT UNIT

The creation of the VIS will require support for:

- The maintenance procedures and daily operation of the VIS;
- The training of Member States users;
- The support of Member States users in using the system (help-desk);
- The maintenance of specific equipment at the consular posts;
- The management of the user access rights;
- The general co-ordination of these new supporting activities.

Technical support units (TSU) should be created at the central (C-VIS) and national (N-VIS) levels. Accordingly, with regard to the new system, and to the allocation of responsibilities between the EC and the Member States, a central TSU (operated at the C-VIS) will be under the responsibility of the relevant organisation and will be in charge of the VIS operation and the training of the Member States.

Member States would be in charge of user management (access rights management of the new system), and of training as well as providing help desk support to the national consular posts and authorities that make use of the VIS.

10.13 SECURITY MEASURES

Security measures to ensure the invulnerability of the VIS have to be introduced. These include the encryption of the biometric templates upon capture, network level encryption to ensure the confidentiality of data, authentication of users, intrusion detection, monitoring and reporting as well as counter-measures in case of altered data.

10.14 COMMON TECHNICAL PLATFORM FOR VIS AND SIS II, COST SAVINGS AND INTEROPERABILITY

With regards to SIS II, interoperability at the functional level would be introduced, as the SIS consultation could be initiated during the visa-issue process within the VIS. SIS II could be consulted during the visa issue procedure for every new visa application. Similarly, the SIS II users could consult the VIS database through the national interface. This type of interoperability shall by no means imply the merging of the two systems.

The existing technology facilitates keeping both systems separated while sharing functionality and data; and at the border-control level no additional equipment would be needed.

It is strongly recommended that common technical standards, development methodologies, and technical platforms be used for both VIS and SIS II. This is a precondition to insuring interoperability between the systems, facilitating the exchange of data and sharing of functionality in order to support the business operations. Moreover this has a significant impact on the financial and human resources required.

APPENDIX A REFERENCE DOCUMENTS – GLOSSARY AND ABBREVIATIONS

A.1 REFERENCE DOCUMENTS

1. The Common Consular Instructions, (Annex 1 to Decision of the Executive Committee of 28 June 1999, OJ L 239 of 22.9.2000, p. 317), amended by
2. Council Decision 2001/329/EC of 24 April 2001 (OJ L 116 of 26.4.2001, p. 32);
3. Council Decision 2001/420/EC of 28 May 2001 (OJ L 150 of 6.6.2001, p. 47);
4. Council Regulation (EC) 539/2001 of 15 March 2001 (OJ L 81 of 21.3.2001, p.1);
5. Council Regulation (EC) 1091/2001 of 28 May 2001 (OJ L 150 of 6.6.2001, p. 4);
6. Council Decision 2002/44/EC of 20 December 2001 (OJ L 20 of 23.1.2001, p. 5);
7. Council Regulation (EC) 334/2002 of 18 February 2002 (OJ L 53 of 23.2.2002, p. 7);
8. The Common Consular Instructions on visas for the diplomatic missions and consular posts, (OJ C 313 of 16.12.2002, p.1);
9. Decisions of the Schengen Executive Committee related in particular to the extension of visas, common principles for cancelling, issuance of visas at the border (OJ L 239 of 22.9.2000, p.151 ff.);
10. Uniform format of a visa application form, introduced by Council Decision N° 2002/354/EC of 25 April 2002 (OJ L 123 of 9.5.2002, p. 50);
11. Information on the criteria and procedures currently used by each Member State to store data on visas (Annex I of the Council guidelines);
12. Statistics on visas provided by the Member States in relation to 2000 and 2001 (Annex II of the Council guidelines);
13. Communication from the Commission to the Council and the European Parliament "Development of the Schengen Information System II" (COM (2001) 720 final;
14. Strategic document of Commission's security service "Information Systems Security Architecture" is under revision;
15. Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations (OJ L 101, 11.4.2001, p. 1);
16. Decision of the Commission 2001/844/EC on Commission provisions on security (OJ L 317, 3.12.2001);
17. BIOMETRIC ASSESSMENT, An evaluation of the potential use of biometric technology by the California Department of Motor Vehicles in the issuance of driver license and identification cards;
18. ARCHITECTURE GUIDELINES for Trans-European Telematics Networks for Administrations – Glossary Version 6.1.;

A.2 GLOSSARY OF COMMONLY USED TERMS

The following terminology has been used throughout the report:

Access	The ability to enter a secured area. The process of interacting with a system. Used either as a verb or as a noun.
Access Control	A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access. The process ensures that systems are only accessed by those authorised to do so, and only in a manner for which they have been authorised.
Application Programming Interface (API)	A set of subroutines or functions that a program, or application, can call to tell the operating system to perform a task.
Audit	The independent examination of records to access their veracity and completeness.
Audit Trail	Audit trails provide a date and time stamped record of a system's usage They record what a computer was used for, allowing a security manager to monitor the actions of every user, and it can help in establishing an alleged fraud or security violation. An audit trail may be on paper or on disk.
Authentication	The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).
Authorisation	The process of determining what types of activities are permitted. Usually, authorisation takes place in the context of authentication. Once you have authenticated a user, the user may be authorised different types of access or activity.
Automated Fingerprint Identification System (AFIS)	A biometric system that compares one or more finger-scan templates with a large database of templates.
Availability	The property that data, information, and information and communications systems are accessible and usable on a timely basis in the required manner.
Backbone	A high-speed line or series of connections that forms a major pathway within a network. The term is relative, as a backbone in a small network will likely be much smaller than many non-backbone lines in a large network. See Also: Network
Background Operation	The name applied to a program running in a multi-tasking environment over which the user has no direct control.
Backup	A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

Bandwidth	The amount of data that can be transmitted in a fixed amount of time. Usually measured, for digital devices, in bits-per-second. A full page of English text is about 16,000 bits. A fast modem can move about 15,000 bits in one second. Digital TV requires 4,000,000 bits per second for normal compression.
Biometrics	The automated use of behavioural or physiological characteristics to identify a person or to verify a claimed identity.
Biometrics Access Control	Any means of controlling access through human measurements, such as fingerprinting, voiceprinting and retina pattern.
Biometric data	Identifiable unprocessed biometric images, such as fingerprint or iris image (referred to as a biometric sample).
Biometric information	A biometric template.
Biometric template generation	Biometric templates, both enrolment and match templates are created through the following process. An individual presents biometric data or biometric sample. Biometric data is processed and filtered to optimise image quality. A feature extraction algorithm locates distinctive characteristics from this sample and converts these features into a template. Enrolment templates are stored for subsequent matching in a biometric system. Matching is the comparison of a match template and an enrolment template. Biometric matches result in a score, which is compared to a threshold to determine whether the two templates match.
Browser	A Client program (software) that is used to look at various kinds of Internet resources. See Also: Client , URL , WWW, Home Page (or Homepage)
Certificate Authority	A certificate authority is a trusted server that maintains and validates digital certificates according to the X.509 standard. A digital certificate uses a public-key encryption scheme to authenticate a particular server or user. Certificates can also prove that a file came from a trusted source and has not been maliciously modified. See also: Security Certificate.
Confidentiality	The property that data or information is not made available or disclosed to non-authorised individuals, entities, or processes.
Cryptographic key	A parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.
Cryptography	The discipline which embodies principles and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.
Data Protection	A group of techniques used to preserve three desirable aspects of data: Confidentiality, Integrity and Availability.
Decryption	Decryption is the process of transforming ciphertext back into plain

	text. It is the reverse of encryption.
Electronic Signature	A means of protecting a message from denial of origination by the sender, usually involving the use of asymmetric encryption to produce an encrypted message or a cryptographic check function.
Encryption	The transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.
Enrolment	The process of providing biometric data for further use in the biometric system.
eXtensible Mark-up Language (XML)	XML is designed to enable the use of SGML on the World Wide Web, although not all browsers support this standard yet. It defines "an extremely simple dialect of SGML which is completely described in the XML Specification. The goal is to enable generic SGML to be served, received, and processed on the similar to HTML".
False Match Rate (FMR)	The probability that an individual's template will be incorrectly determined to be a match for a different individual's template. In a One-to-One system, FMR is the probability that an individual will be verified as another individual. In the One-to-Many system, FMR is the likelihood that an individual is correctly identified as another individual.
False Non-Match Rate (FNMR)	The probability that an individual's template will be incorrectly determined to not match the individual's existing template. In a One-to-One system, FMR is the probability that an individual will not verify against his or her own template. In the One-to-Many system, FMR is the probability that an individual enrolled in the database will not be identified in a search.
Failure to Enrol (FTE) Rate	The likelihood that a given individual will be unable to enrol in a biometric system.
Feature extraction	The process of locating and encoding distinctive features in order to create a template from identifiable biometric data.
File Compression	The compacting of a file through the process of recording its bit structure into a shorter form. File compression must be reversible.
File Server	A central data repository for a computer network, which may provide other central services such as shared printer control.
Hypertext Markup Language	An ASCII text based, scriptlike language for creating hypertext documents like those on the Internet's World Wide Web.
Hyper Text Transfer Protocol	The protocol used between web server and web browsers on the World Wide Web.
Identification	The process of determining a person's identity through a database search against multiple templates. It is referred to as One-to-Many, in which "N" represents a variable of unknown size.

Integrity	The property that data or information has not been modified or altered in an unauthorised manner.
Internet Protocol	See also TCP/IP
Intrusion Detection	Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.
Key	In encryption, a key is a sequence of characters used by an encryption algorithm to transform plain text data into encrypted (ciphertext) data, and vice versa. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilised to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected, software.
Leased-line	Refers to a phone line that is rented for exclusive 24-hour, 7-days-a-week use from your location to another location. The highest speed data connections require a leased line.
Log Processing	How audit logs are processed, searched for key events, or summarised.
Log Retention	How long audit logs are retained and maintained.
Logging	The process of storing information about events that occurred on the firewall or network.
Matching	The comparison of a biometric template through an algorithm to determine their degree of similarity. In most systems, a biometric match produces a score, which is compared against a threshold.
Mirror	Generally speaking, to mirror is to maintain an exact copy of something. Probably the most common use of the term on the Internet refers to mirror sites which are web sites, or FTP sites that maintain exact copies of material originated at another location, usually in order to provide more widespread access to the resource. Another common use of the term mirror refers to an arrangement where information is written to more than one hard disk simultaneously, so that if one disk fails, the computer keeps on working without losing any data.
Mirroring	A technique where data is written to two (or more) disks simultaneously, with the intention of enabling data retrieval even when one of the disks fails.
Non-repudiation	A property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or

	for proof of ownership).
Private Key	Symmetric cryptographic systems use a single key, the private or secret key, both to encrypt and decrypt data.
Public Key	Asymmetric cryptographic systems use two keys, a public key (publicly available) and a private (secret) key to encrypt and decrypt messages. The mathematical relationship between the two keys is such that knowledge of one key cannot be used to deduce the other. Thus, one key (the public key) can be made publicly available while the other (the private key) remains secret.
Router	A special-purpose computer (or software package) that handles the connection between 2 or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding which route to send them on.
Security	Protection against unwanted behaviour. The most widely used definition of (computer) security is security = confidentiality + integrity + availability.
Security Certificate	An electronic file commonly used to authenticate the identity of the sender of a message, and to provide the recipient with the means to encrypt a reply. The certificate is used by the SSL protocol to establish a secure connection. Security certificates contain information concerning what it belongs to, who issued it, a unique serial number or other unique identification, valid dates. In order for an SSL connection to be created both sides must have a valid Security certificate.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running. A single server machine could have several different server software packages running on it, thus providing many different servers to clients on the network.
Smart Card	A credit-card-sized device with embedded micro-electronic circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Template	Distinctive encoded files derived from the unique features of a biometric sample or biometric data. Templates exist as enrolment templates, those created and stored when enrolling in the system, and as match templates, those generated during subsequent verification and identification attempts.
Threshold	The score above or below which a match/no match decision is made.
Transmission Control Protocol / Internet Protocol (TCP/IP)	A set of communication protocols developed by the U.S. Department of Defence that allows dissimilar computers to share information over a network. TCP/IP is the transmission protocol used by the Internet.

Verification (Authentication)	A comparison of two templates to establish the validity of a claimed identity. This is a One-to-One match. *Authentication* is the process of claiming an identity and subsequently verifying the claimed identity.
Virtual Network Perimeter	A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over non trusted networks.
Wide Area Network	Pronounced "WAN" to rhyme with "LAN". A geographically dispersed network formed by linking several computers or local area networks (LANs) together over long distances, usually using leased long distance lines. WANs can connect systems across town, in different cities, or in different regions of the world.
World Wide Web	A collection of richly formatted hypertext "pages" located on computers around the world and logically linked together by the Internet. With a graphical Web browser users can "surf" the Web by clicking highlighted words on the screen. Each click activates a hypertext link, connecting the user to another Web location identified by a URL. See also HTML and URL.

A.3 ABBREVIATIONS

The following abbreviations have been used throughout the report:

ACL	Access Control List
API	Application Programming Interface
BCS	Business Continuity System
CP	Consular Post
CUG	Closed User Group
C-VIS	Central Visa Information System
CS	Core System (SIS II)
DNS	Domain Name Server
EC	European Commission
(E)SMTP	(Extended) Simple Mail Transfer Protocol
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
ICAO	International Civil Aviation Organisation
IP	Internet Protocol
IS	Information System
ISP	Internet Service Provider
IT	Information Technologies
JBIG2	Joint bi-level image Experts Group
JPEG	Joint Photographic Experts Group

Kbps	Kilobits per second (kilo = 1000 bits)
Mbps	Megabits per second (Mega = 1,000,000 bits)
MS	Member State
NCA	National Central Authority
NI	National Interface (SIS II)
N-VIS	National Visa Information System
PIB	Police, Immigration and Border checkpoint authorities
PKI	Public Key Infrastructure
SLA	Service Level Agreement
SIS II	Schengen Information System II
SISNET	Schengen Information System Network
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
SWOT	Strengths, Weaknesses, Opportunities, Threats
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TESTA	Trans European Services for Telematics between Administrations
TSU	Technical Support Unit
UTF	Universal Multiple-octet coded character set Transformation Format
VIS	Visa Information System
VISION	VIS Inquiry Open-border Network
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web
XMI	XML Metadata Interchange
XML	EXtensible Mark-up Language

APPENDIX B : ANALYSIS OF VIS BUSINESS PROCESSES

The section introduces the visa issuing and VIS consultation process providing details on the application of VIS in the following processes:

1. New visa without a previous registration;
2. New visa with a previous registration;
3. Visa and traveller verification;
4. Person identification;
5. The existing VISION consultation functionality (refer to Annex C);
6. SIS II consultation (during visa issuance, entry and exit);
7. Reporting, statistics and maintenance.

Visa issuing process deals with visa application *registration*, *assessment* and visa issuing *decision*. Supported functions include electronic registration and enrolment of the visa application, applicant verification (for regular travellers previously registered in the system) or negative identification (for newly enrolled travellers applying for a visa for the first time). The management of the visa application status (e.g. granted, refused, under consultation) concludes the visa issuing process.

VIS consultation involves obtaining information from the applicant (traveller), followed by *assessment* and the final *decision.* Supported functions includes verification (documented persons) and/or identification (undocumented or suspected persons). Identification, depending on the use, is divided into *positive identification* and *negative identification*. Positive identification is performed by police or immigration authorities (as a result of a failed verification) to determine the identity of an undocumented person. Negative identification is performed during the visa issuing procedure for all the applicants applying for a visa for the first time. This helps to avoid enrolling the same applicant twice in the system under two different identities [28].

New visa without previous VIS registration:

Each new visa application form and the particulars of the applicant could be electronically registered in the VIS. This includes alphanumeric data (drawn from the visa application form), photograph, biometric data and supplementary documents accompanying the visa application. A negative identification would be conducted to verify that an applicant has not been enrolled twice under two different identities. If the result of the negative identification provides no match with the VIS database and the person is bona fide the visa could be issued. If a match to an existing VIS applicant (record) is found, the new visa application/applicant should not be enrolled into VIS until further screening is performed to determine the true and unique identity of the traveller.

[28] For further information refer to the section on the application of biometrics in the VIS business processes.

New visa with previous VIS registration:

The process assumes that an applicant has applied for a visa in the past and is thus known (registered) in the VIS. The visa sticker could be used as the key to retrieve the personal particulars, the visa history and the photograph stored in the VIS database. The person's identity is verified against the information retrieved from the system. A simple visual verification (bona-fide traveller) can be performed comparing the traveller to the photograph stored in VIS.

Once biometric systems are readily available in consular missions, identity verification would be performed through the comparison of the enrolled template and the live biometric obtained from the applicant.

Visa and traveller verification:

The process is mainly performed at border checkpoints. To a lesser extent, it is also used by police and immigration authorities to verify the identity of documented persons. It aims to verify that the carrier and the holder of the visa are the same person.

Two options are available to support visa and traveller verification:

1. On-line verification through the VIS;

2. Off-line verification with a portable (handheld) device without connectivity to the VIS.

In the on-line verification, the visa sticker could be used as the key to retrieve information from the VIS to verify that the carrier and the holder of the visa are the same person. Alternatively, biometrics could be used to verify the identity of the traveller against the VIS and retrieve the visa sticker information for further verification (carrier is the holder).

Off-line verification could be performed using a handheld device such as a standard pocket computer equipped with a barcode reader, biometric acquisition device and software. This option assumes the use of smart cards or PDF barcodes to securely store biometric data (and visa sticker information). A border checkpoint officer uses the portable device to acquire traveller's biometric data and read the information stored in the smart card or PDF. The device compares the two digital patterns for a possible match. This would verify the identity of the traveller, the validity and integrity of the visa sticker, and that the carrier and the holder are indeed the same person.

Person identification (positive/negative):

Negative identification is performed during the enrolment of all the applicants applying for a visa for the first time. The purpose is to avoid having enrolled the same person twice in the system under two different identities (and visa histories).

Positive identification is performed by police and immigration officers (possibly as a consequence of a failed verification) to determine the identities of undocumented persons.

Reporting, statistics and maintenance:

VIS will facilitate production of statistical reports primarily targeted to central national authorities.

Detailed information concerning the business processes from a system point of view is provided below.

B.1 1 NEW VISA WITHOUT PREVIOUS REGISTRATION

Purpose: To register a new visa application and the applicant's particulars in the VIS database, and to subsequently manage the status of the visa application. Every new applicant has to be negatively identified against the VIS enrolees. If there is no hit or if there is no reason to refuse the VISA, the visa could be issued. The identification could also be used to prevent VISA shopping.

Input data: Data drawn from the uniform visa application form including the ID number of the visa application form, a photograph, biometric data and supplementary documents.

Output data: A confirmation from the system with two unique keys:

a) the ID number of the applicant;

b) the visa sticker number (if visa is delivered).

Processing: A request (electronic form) is prepared and submitted to the VIS with the input data. The request feeds the trial template to the biometric matching engine to carry out a negative identification. If no match is found between the applicant's template and that of an existing enrolee, the new records are automatically enrolled in the database(s). If a match is found between the applicant's template and that of an existing enrolee, the new records are registered (and not enrolled) in the database and the applicant will have to be screened against the database hit. A visa would not be issued and the visa application remains registered in the VIS to prevent visa shopping.

If a biometric sub-system is not available, negative identification could not be performed using the information encoded in the uniform visa application form (e.g. name, surname, gender, and approximate age etc.). In this case, the alphanumeric database will be queried for possible matches (fuzzy search).

Comments: The common European VIS application should integrate a unique ID number.

Performing alphanumeric identifications is not efficient, the search engine could return long lists of candidates matching the applicant and heavy screening would have to be carried out (becomes nearly impractical). Only biometric techniques can determine an identity with certainty.

B.2 NEW VISA WITH PREVIOUS REGISTRATION

Purpose: To register in the VIS system a new visa request that pertains to a known applicant (applicant has previously registered in the VIS). Subsequently manage the status of the visa application. It is feasible to authenticate the applicant against the existing VIS database information. If verification is successful, the visa will be granted.

Input data: Data drawn from the uniform visa application form including the ID number of the visa application form, a photograph, biometric data and the supplementary documents.

Output data: A confirmation from the system with two unique keys:

a) the ID number of the existing applicant;

b) the visa sticker number (if visa is delivered).

Processing: A request (electronic form) is prepared and submitted to the VIS with the input data. The request feeds the trial template to the biometric matching engine to carry out the

verification. If the verification is successful the new records are automatically enrolled in the database(s). A specific flag indicates the status of the applicant/application. If the verification fails, a visa will not be issued and the visa application remains registered in the VIS to prevent visa shopping.

If a biometric sub-system is not available, verification will be performed using the visa sticker number. Photograph and other alphanumeric data returned by the search engine would be used to verify the applicant.

Comments: The common European application should integrate a unique ID number.

B.3 VISA AND TRAVELLER VERIFICATION

Purpose: Facilitate checks that the carrier and the holder of the visa are the same person, at external borders or at immigration or police checkpoints.

Input data: Visa sticker number, biometric data.

Output data: Valid visa (Yes or No), carrier is the holder.

Processing: If a biometric sub-system is not available, the verification process will rely on alphanumeric data. The visa sticker number is keyed-in and the sticker is validated against its image stored in the VIS. The visa sticker data and the photograph of the carrier are retrieved from the VIS database. The carrier is verified against the VIS database information (valid sticker validation, verification that the carrier is the holder).

If a biometric sub-system is available, the carrier's trial template (visa carrier) and the biometric template linked to the visa sticker (visa holder) are compared by the biometric engine. If they match, the visa sticker is authentic and carrier is the holder.

Comments: Verification can also be performed in *off-line* mode without connecting to the VIS. The biometric reference templates (and visa sticker information) are securely stored (encrypted) and digitally signed in a storage device such as a chip card or paper document.

Performing alphanumeric verifications could become impractical as the VIS database grows over time. The search engine could return long lists of candidates matching the applicant and heavy screening would have to be carried out. Only biometric techniques can determine an identity with certainty and within the required response times.

B.4 PERSON IDENTIFICATION (POSITIVE/NEGATIVE)

Purpose: Contribute towards internal security and the combating of terrorism. In that respect:

1. *Positive identification* could facilitate the application of the Dublin Convention in determining the State responsible for examining applications for asylum and, could assist in the identification and documentation of undocumented illegals and, could simplify the administrative procedures for returning citizens of third countries and identify bona fide travellers with lost/stolen documents;

2. *Negative identification* (during enrolment) could be carried out for all travellers applying for a visa for the first time. The purpose is to avoid enrolling the same applicant twice in the system under two different identities (and visa histories).

Input data: Biometric data, gender, other information if available.

Output data: Identity (including all the information available).

Processing: If a biometric sub-system is not available, the available alphanumeric data is submitted electronically to the VIS to carry the One-to-Many search (against the existing alphanumeric database) for possible matches. Photographs returned by the system could be used to screen the results and determine the identity.

If a biometric sub-system is available, the trial template is submitted to the biometric engine, which carries a One-to-Many search against the existing enrolee templates for a possible match. Similarly, photographs returned by the system will be used to screen the results and determine the identity.

In both cases the VIS aids to determine the identity of a person, if this person had applied for a visa before.

Comments: Performing alphanumeric identifications is totally impractical. The search engine could return long lists of candidates matching the applicant and heavy screening would have to be carried out. Only biometric techniques can determine an identity with certainty and within the required response times.

B.5 REPORTING, STATISTICS AND MAINTENANCE

Purpose: Reporting statistics of the VISA process for the Member States, including maintenance and update of information.

Input data: Country, administration, geographical region, type of visa, visa status etc.

Output data: VIS will support the automated production of statistics, which include[29]:

a) Statistics per country on the visas issued, refused, revoked, extended, annulled;

b) Comparison charts per country;

c) Per visa status (issued, refused, revoked, extended, annulled)

d) The applicant's country of origin;

e) Global statistics per geographic region and even per consulate.

[29] A large number of statistic reports can be provided by VIS system – as part of an automated reporting and statistics application service. The ones hereunder are indicative examples.

APPENDIX C : VIS AND VISION INTEGRATION

C.1 BACKGROUND INFORMATION

One of the objectives laid down in the Convention implementing the Schengen Agreement is the establishment of a consultation network between the central authorities of the partner states for visa applications made by nationals from sensitive areas. **This electronic consultation network** – known as VISION Network - **VIS**a **I**nquiry **O**pen-border **N**etwork was established through close-collaboration of the Ministries of Foreign Affairs of the countries involved.

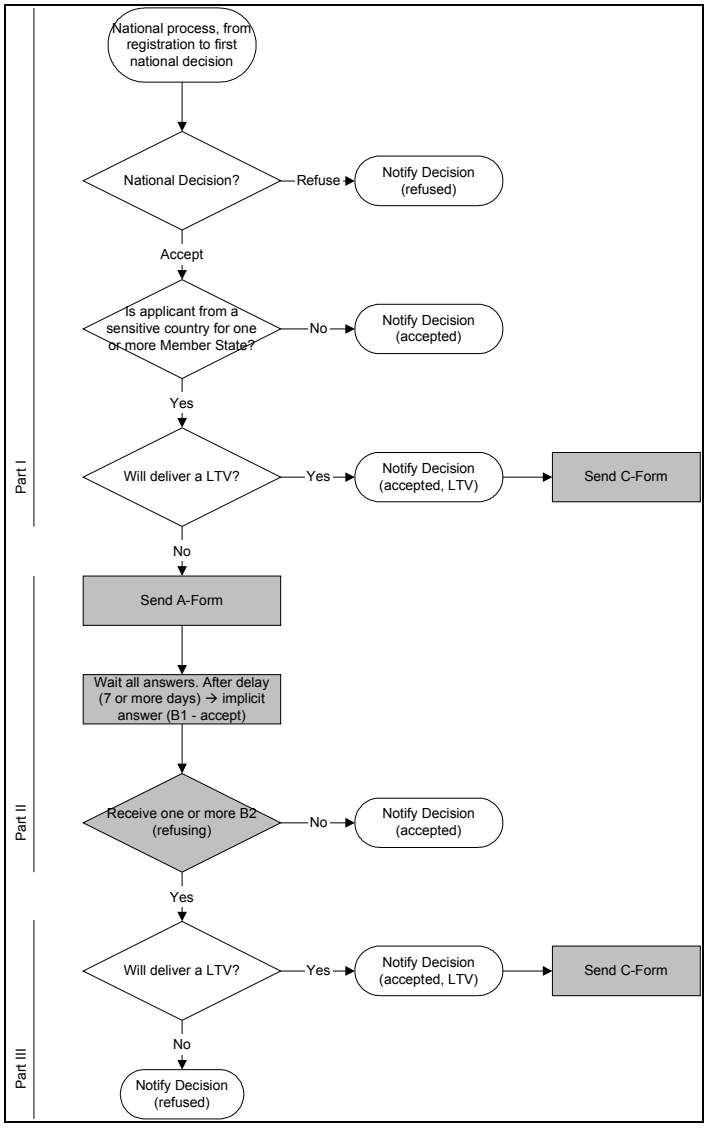
From a technical perspective, VISION is a message exchanging system[30]. It supports the electronic exchange of six types of message (referred in the VISION notation as Forms):

- Form A - Consultation request regarding VISA application;
- Form B - Reply to consultation request (B_1 - explicit approval, B_2 - refusal, B_3 and B_4 - request to extend the deadline);
- Form C - Notification of issue of VLTV;
- Form E - Error message;
- Form F - VISA application within the framework of Representation;
- Form G - Response to a VISA application within the framework of Representation.

Figure 10-1 illustrates the VISION consultation process. The process is initiated by visa issuing authorities for aliens (visa applicants) where their country of origin is in the list of "sensitive"[31] countries as these have been declared by Member States, in appendix 5B of "Common Consular Instructions on Visas".

[30] VISION is base on the X.400(88) protocol.
[31] For non-sensitive countries, VISION is not invoked.

Figure 10-1: VISION consultation.



Referring to the above figure:

Part I deals with the visa issuing process, from the time an alien lodges a visa application with a diplomatic mission. Prior to any communication/consultation with the Member States[32] according to the provisions stated in appendix 5B of "Common Consular Instructions on Visas", a Member State can exercise its right to deliver an VLTV.

Part II implements the VISION consultation process: The diplomatic mission disseminates the A-Form to one or more Member States, according to appendix 5B of "Common Consular Instructions on Visas". The consulted country/countries will communicate their decision to grant or refuse a visa to the diplomatic mission through B-Form.

Part III deals with the special case where one or more of the consulted countries refuse to grant a visa. In this case the visa issuing authority may decide to grant and deliver a VLTV.

[32] This is a practical point of view. If Visa issuance authority decides to refuse, they don't have to consult other Member States. In the same manner, if they decide to deliver a VLTV for specific reasons, no consultation is needed, only a direct notification of VLTV.

With regard to the previous business processes and operations, there are synergies between VIS and VISION, the development of the former could have an impact on the latter. Both systems share similar data (visa applications) and have message type application architectures. This qualifies the VIS and VISION integration as a candidate option.

Two options have been analysed:

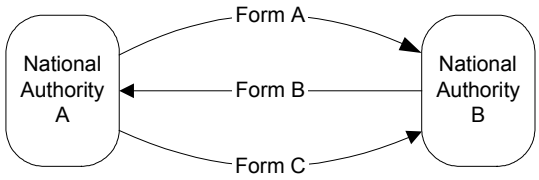
Option 1: Integration of the VISION and VIS services. VISION services may use the VIS database services. VISION consultation is implemented against the VIS data repository;

Option 2: Develop VIS service to provide the VISION consultation.

C.1.1 Option 1: Integration of VIS and VISION services

Figure 10-2 illustrates a typical VISION consultation between two Members States.

Figure 10-2: Typical peer-to-peer VISION consultation



The information (data) included in A-Form and C-Form is a sub-set of the data stored in the VIS database. Therefore, VISION consultation may draw data stored in the VIS database. VISION messages will embed URL like links to the VIS data repository to facilitate information retrieval. Informative decisions on visa applications according to the provisions stated in appendix 5B of "Common Consular Instructions on Visas" will be performed against VIS data.

Advantages/Disadvantages:

(++) Reduce the VISION network traffic;

(+) Improve the quality of information. The A-Form information is a subset of the Uniform Visa Application Form. VISION supports ASCII character encoding which provides very poor searching capabilities. VISION users can access the full set of VIS information, including increasing the effectiveness of the control;

(-) The VISION application will need to be further developed;

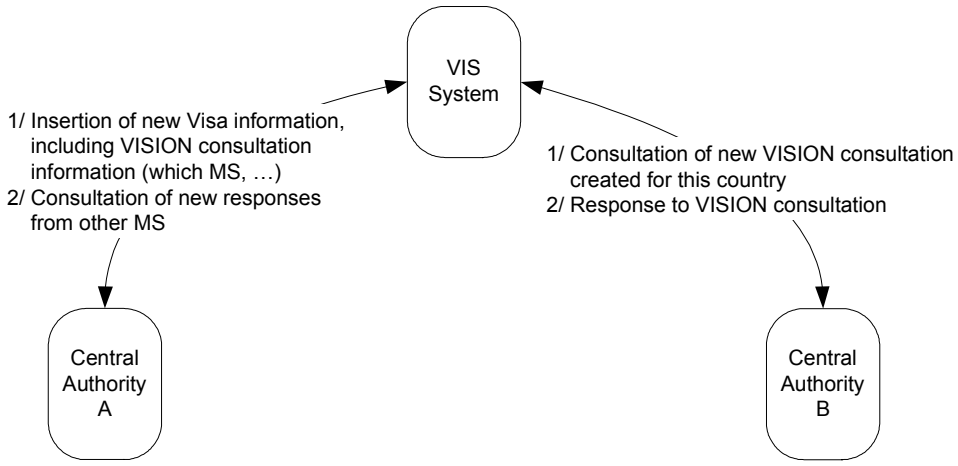
(-) Build a legal framework to “grant” VISION access to VIS information;

(-) Increased support and maintenance costs (both VIS and VISION systems).

C.1.2 Option 2: Develop VISION into VIS

VISION functionalities can be developed in the VIS, making the VISION Network obsolete in the long run (once VIS is readily available). This option requires some re-engineering in the VIS database, and the development of additional services on the VIS application to support VISION functions. The option renders the peer-to-peer communication between the NCAs obsolete. The VIS will support VISION users.

Figure 10-3: VISION consultation implemented through VIS.



Advantages/Disadvantages:

(+++) The VISION Network capacity can be vested in the long run to the VIS services;

(+++) Improve the quality of information. The A-Form information is a subset of the Uniform Visa Application Form. VISION supports ASCII character encoding which provides very poor searching capabilities. VISION users can access the full set of VIS information, increasing the effectiveness of the control;

(+++) Merging VISION and VIS systems will significantly reduce maintenance, administration, testing and deployment costs;

(+++) Both VISION and VIS pertain to the same legal framework (Common Consular Instruction). Integration is easier from a legal perspective;

(+) Easy to introduce new Member States to a unified environment that provides both VIS and VISION services integrated in a single application;

(-) Need to develop a few additional services and enhance the VIS database with some additional tables. Specifications to be developed for the VISION functionalities.

C.1.3 Benchmarking - Financial impact

Option 2 is preferred when considering the VISION and VIS integration. It is easy to implement from a technical perspective through unification of services (VIS and VISION services) over a single application environment. The benefits outperform by far any shortcomings. By fractionally increasing the investment in the VIS application development, the VISION functionality can be provided via VIS[33]. Cost savings in system and application maintenance and support, as a result of having one system, counterbalances this increase in capital expenditure. The table below provides an overview of the financial impact.

[33] The impact on network bandwidth and storage is negligible when considering the global envelope of VIS volumes.

		Cost (Euro)	
Cost Type	**Cost Item**	**Fixed**	**Yearly**
Expense	1. Application development and maintenance (VIS)	-100,000	-100,000
	2. Additional costs (H/W resources, storage, Network)		-200,000
Saving	3. VISION Application maintenance		+300,000
	4. System costs (H/W and S/W)	+1,200,000	
	5. Systems maintenance		+100,000
	6. Systems operations		+200,000
	Total shortfall/surplus	+1,100,000	+300,000

Legend:

1. *Application development and maintenance (VIS):* this is the cost to develop VISION services into VIS. It is estimated at 100,000 Euro;

2. *Additional costs (H/W resources, storage, Network):* Additional investments in hardware resources as a result of additional load into VIS. It is estimated at 200,000 Euro;

3. *VISION Application maintenance:* Saving from ceasing the maintenance of the VISION application. It is estimated at 300,000 Euro;

4. *System costs (H/W and S/W):* Saving from making re-usable hardware resources vested to run the VISION application. It is estimated at 1,200,000 Euro;

5. *Systems maintenance:* Savings in terms of maintenance. It is estimated at 100,000 Euro;

6. *Systems operations:* Savings from freeing resources vested in the VISION system operations. It is estimated at 200,000 Euro (3 man months at a rate of 43,000 Euro for national Expert, scaled for the 15 Member States).

Option 2 creates a surplus of 1.1 million Euro in fixed costs with annual savings of 300,000 Euro. The financial benefits (mainly cost saving in maintenance and support) are significantly higher compared to the initial investment for application development.

APPENDIX D : TECHNICAL SU P PORT UNIT (TSU)

In this chapter we define what could be the role of the **Technical Support Unit (TSU**) within the business context of the VIS, detail the operations and the procedures executed by the TSU, and describe the factors to be considered during the setting up of these units.

D.1 INTRODUCTION

Organisations in charge of managing the VIS need to put procedures in place to ensure the high availability of services and business continuity. These organisations could provide resources to apply preventive measures including implementation of rigorous organisational procedures (systems maintenance procedures, continuous system monitoring, and implementation of the procedures laid down in the business continuity plans…). Moreover, organisations need to participate in an efficient collaboration framework among the central system (C-VIS) and the national systems (N-VIS).

In view of this, **TSUs** should be established at C-VIS and N-VIS, which are in charge of managing the VIS components, to prevent interruption of VIS services (insure business continuity), and to re-establish full functioning as swiftly and as smoothly as possible. For simplicity, the TSU supporting the C-VIS will be referred to as Central-TSU (central technical support unit), whereas the TSU supporting the N-VIS will be referred to as the National-TSU (national technical support unit). The TSUs would have to be established by the organisations in charge of the VIS operation.

A definition for the TSU is as follows: *It is a unit (team of experts) in charge of running the VIS maintenance and operations. The unit provides management services, information facilitation, help-desk and training services with regards to the VIS. It is a centre of technology support and facilitation concerning the VIS.*

D.1.1 Roles and responsibilities

In terms of co-ordination, management and supervision services the TSU:

- Collaborates closely with national authorities (users of the VIS) and the central authorities (providers of the VIS) so as to maximise the impact of the VIS at national level;
- Acts as the manager of the VIS maintenance contracts in close collaboration with vendors and service suppliers to ensure alignment of the operations with the objectives of the business continuity planning;
- Supervises technical teams in charge of the system maintenance and operations as well as overseeing help-desk and training services to ensure business continuity on the one hand and maximise the impact of the new system on existing operations on the other.

At technical support level, the TSU provides:

- System configuration and maintenance (updates/upgrades of hardware and software);
- System management and monitoring;
- System performance monitoring, analyses and reporting;
- Implementation of back-up and archiving policies;
- Manage unplanned service outages (failures) with a view to maintaining business continuity;

- Implement, review the business continuity policies as well as testing the business continuity systems.

At the administrative support level, the TSU provides:

- Help desk support;
- Training support.

D.1.2 Central (C-VIS) Technical Support Unit

The **Central-TSU** would perform the following tasks:

1. Co-ordinate at Trans-National level between the authority operating the central visa information system (C-VIS) and the national authorities in charge of the national visa information system (N-VIS);

2. Operate, manage and maintain the C-VIS, implement the back-up and archiving policies, perform hardware and software upgrades and updates, perform system performance analyses and operations reporting, central level user access management as well as implementing, reviewing and testing the business continuity policies;

3. Provide training to:

- The operators (technical experts) in charge of the maintenance and technical support operations at the N-VIS;
- The team of trainers that has to train national trainers.

The training could concern the latest developments and upgrades of the VIS as well as the sharing of best practices sharing. The latter aims to facilitate technical co-operation between the central and national technical teams in charge of the operations of the C-VIS and N-VIS respectively.

D.1.3 National (N-VIS) Technical Support Unit

The **National-TSU** could be in charge of the following tasks:

1. The Co-ordination at National level, between the authorities in charge of the national visa information system (N-VIS) and other national authorities, which make use of the VIS, services (e.g. police, immigration authorities). National user access management also falls under this domain of responsibility;

2. Perform the N-VIS systems operations and management, system maintenance as well as testing the business continuity systems.

The unit shall also:

- Provide help-desk and end-user training services to the VIS users, such as consular posts, border-crossing authorities, etc (e.g. all the national VIS users);
- Act as the co-ordination centre for the technical problems encountered by the national VIS authorities and their users. Technical problems at the diplomatic missions and consular posts could be registered at the help desk operated by the National-TSU, which would be in charge of resolving the problem in close collaboration with the hardware and software vendors.

Diplomatic missions or consular posts (category III) may also consider assigning a person in charge of the technical support at local level. This could facilitate the enhanced co-ordination between the local and the National-TSU. Problems at local level would be relayed (from consulate) and registered to the help-desk operated at national level (National-TSU).

D.1.4 Synthesis

The table hereunder provides the synthesis of the activities that could be performed by the Central (C-VIS) and National (N-VIS) Technical Support Units. Activities have been split into three domains: *Co-ordination and management* and *administrative support*.

TECHNICAL SUPPORT UNITS (TSU)	
Central (C-VIS)	**National (N-VIS)**
Co-ordination and management: – Management of maintenance contracts of the central systems (C-VIS) – Supervision of the technical support services at the C-VIS – Management of the access rights policy at central level according to central policies and clearance procedures – Management of the VIS business continuity planning including testing and reporting; – Network contract management.	**Co-ordination and management:** – Management of the maintenance contracts of the national systems (N-VIS) – Supervision of technical support services at the N-VIS – Management of the access rights policy at national level according to national policies and clearance procedures – Management of the N-VIS business continuity planning including testing and reporting;
Administrative support: – Member State training at the following level: – Training of the personnel in charge of providing technical support at national level – Training of the personnel in charge of providing end-user help desk support at national level – Training of the persons in charge of providing training at the diplomatic missions and consulates.	**Administrative support:** – Help Desk support (consulates and national users); – Training consulates and other national users to use and operate the standard configurations.

Appropriately skilled personnel should run the above operations. The investment and resource planning of chapter 7 includes provisions for these human resources.

Below, details are provided with regards to the technical and administrative procedures to be applied by the Technical Support Units.

D.2 TECHNICAL SUPPORT PROCEDURES

All the TSUs should implement a comprehensive set of planned controls and measures to prevent interruption of the VIS services. In addition, they should deal with unplanned events (e.g. sudden system failure) in order to re-establish full functioning as swiftly and as smoothly as possible.

D.2.1 System management

Systems management should be as fully automated as possible, using monitoring tools. The role of the TSUs could be limited to:

1. Perform 24h/7d surveillance of the control monitors provided by the system management software;

2. Analyse encountered problems and apply the procedures laid-down in the business continuity planning;

3. Monitor the switch-over from the production environment to the fail-over system in the event of disaster (business discontinuity);

4. Initiate maintenance/repair requests with the vendors in the event of failures;

5. Perform analysis of the system log files and provide reporting concerning the VIS system usage;

6. Test business continuity plans and, in particular, assess the readiness of redundant systems and sub-systems to assume full functioning in the event of system failure.

D.2.2 System monitoring

The VIS should be continuously monitored (365/7d/24h) through a distributed monitoring system. This system would provide a range of monitors for the operating system parameters, network parameters and application parameters.

The TSUs should manage the alerts generated by the monitoring system as follows:

1. Provide 24h/7d surveillance of the distributed monitoring system and to monitor how a system or application meets Service Level Agreements (SLAs);

2. Respond to alerts initiated by the monitoring system, assess the impact of the alerts on the continuity of the system and apply the necessary business continuity procedures;

3. Initiate maintenance/repair requests with the vendors in the event of a system failure;

4. Document of system alerts, their impacts on the business and the measures that have been taken to resolve the incidents;

5. Review the business continuity planning concerning system monitoring.

D.2.3 System maintenance and change management

The TSUs would be in charge of the following planned events:

1. To implement VIS maintenance procedures in view to ensure the high availability of the VIS system, and

2. To administer changes in the VIS environments (applications, databases, and network configurations) that could potentially affect the business continuity of the system. Such planned changes could come from various sources:
   - Software environment changes:
     - Operating system upgrades.
   - Application software changes:
     - Development of new functionalities (or integration between VIS and an existing National legacy system).
   - Hardware configuration changes:
     - Changes to the current hardware configuration at the C-VIS or N-VIS;
     - Scaling.
   - Changes to the networking environment;
   - Organisational changes at C-VIS or N-VIS;
   - System configuration changes (hardware upgrade).

3. To perform business impact analysis in order to determine the impacts associated with disruption to specific functions due to change management process;

4. To review the change management procedure as a result of the business impact analysis;

5. To document the results of the change management procedures.

D.2.4 Back-up and archiving policies

Back-up and archiving operations would be automated using appropriate scheduling software. The TSU's role could thus be confined to:

1. Provide 24h/7d surveillance of the execution of the back-up and archiving policy;

2. Implement data recovery operations in the event of a failure according to the procedures laid down in the business continuity plans and the data recovery sequence priorities;

3. Constantly review the back up and archiving policies, laid down in the business continuity planning, in view to meet the business continuity requirements.

D.3 ADMINISTRATIVE SUPPORT

D.3.1 Help desk support

A help desk should be operated by the Member States in order to support their diplomatic missions and consular posts and other national authorities with access to the VIS. The help desk

line would have to be manned by experts trained to support the VIS systems and operating procedures performed by the visa issuing offices.

D.3.2 Training

Training should be provided at central (C-VIS), national (N-VIS) and local level by relevant organisations.