5. CANDIDATE ARCHITECTURES

5.1 THE SYSTEM ARCHITECTURE

The system architecture defines the organisation of the VIS. It aims to provide, from a technical standpoint, an overview of the major components and interfaces of the VIS including their characteristics. In the context of the VIS, the architecture is based on the functional technical and operational requirements, the business model and the biometric considerations that have already been addressed beforehand in this document.

In particular, system architecture describes:

1. The architecture of the data components (alphanumeric, photo, biometric and supporting documents) to be stored and processed by the system;

2. The organisation of the business processes and functions that serve the VIS business context;

3. The information flows that pertain to the business processes (visa issue, visa and traveller verification and person identification).

5.2 BACKGROUND

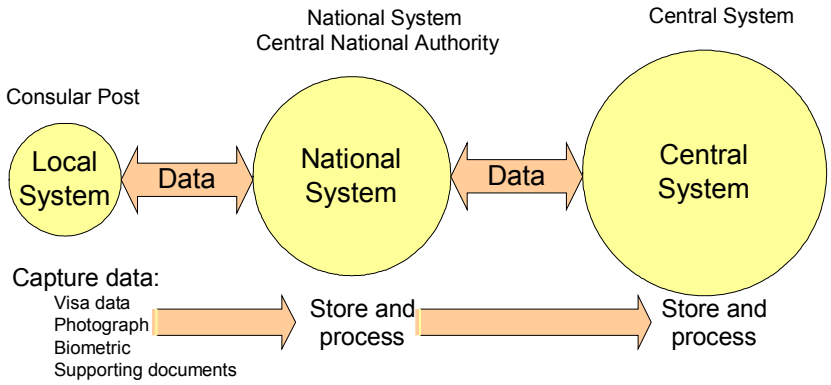
Having regard to the Council guidelines, the structure of the VIS must be similar to that of the existing Schengen Information System (SIS). In view of this, Figure 5-1 illustrates the high level architecture for the VIS. It comprises of:

1. A **Central System**;

2. The **National System**, that describes the VIS services at national level;

3. The **Local systems** at diplomatic missions and consular posts connected to the National System. Visa issue authorities capture visa data, prepare the electronic "visa dossier" and subsequently transmit it to the national and to the central system for storage and processing.

Figure 5-1: High level view of the VIS.



Having taken this generic approach, the obvious question is **what will be the role of the existing national visa systems operated by the Member States in view of the VIS system?**

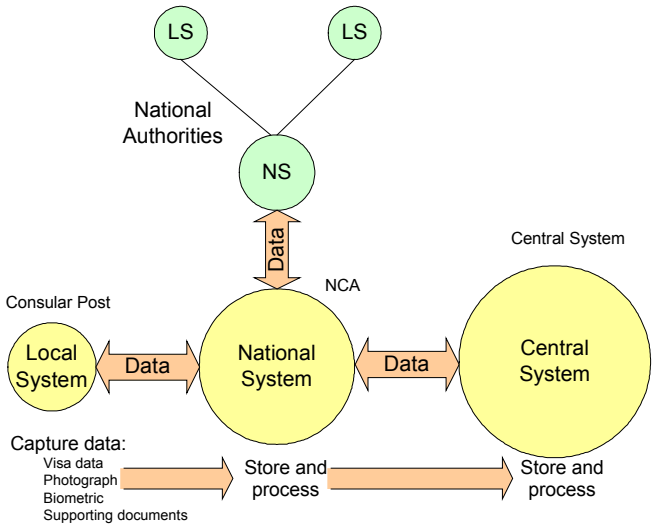
At the present time there is no European-wide information system for the exchange of visa data between the Member States. Some Member States, however, operate national visa systems connecting their world-wide diplomatic missions and consular posts. **What will be the role of these systems in view of the VIS?**

Member States with existing national systems (NS) that have links to their consular posts will also need to connect these national visa systems to the VIS to benefit from its functionalities.

As a result of the VIS open technical standards, Member States could envisage connecting other national systems (e.g. immigration or police) to the VIS, with a view to benefiting from its services (e.g. verification and identification).

This is illustrated in Figure 5-2, which is an elaboration of the VIS architecture from the perspective of interconnecting an existing national system. Note that the existing national system (NS) directly connects to the national component of the VIS, thus interoperability is being accounted for in the VIS.

Figure 5-2: High level view of the VIS with a national perspective.



Legend:
LS refers to an existing **L**ocal **S**ystem connecting to the NS
NS refers to an existing **N**ational **S**ystem operated by the Member States (e.g. an existing national visa system).
NCA refers to National Central Authority.

With regards to Figure 5-1 and Figure 5-2 and in consideration of the guidelines drawn up by the Council the current chapter examines the following two basic options for the VIS:

- **Option 1** concerns a separate VIS system based on the structure of the SIS. For this option, a number of technical solutions for the architecture of VIS are introduced and analysed layer-by-layer, starting from the description of the architecture, its impact on the business information flows, data storage, functionality, communication and technical infrastructure;
- **Option 2** concerns the technical integration of VIS and SIS II. In the second option, the possible synergies between VIS and SIS II are analysed. Synergies are discussed from an operational, functional and technical point of view in order to minimise the human and financial resources required.

Before examining the options in detail, some background information is provided to help with the understanding of the differences between the various architectures. In particular, the terms *data* and *index* are defined and the notion of functionalities (processes) supported by the system is explained in the context of VIS.

5.3 GENERIC ARCHITECTURES

5.3.1 System considerations – Data and function perspective

The VIS architecture comprises a number of databases, each fine-tuned to store and manage a specific data type. Each of these databases stores “data” and “indexes”. An "Index" refers to information stored in a database that is available for a search. "Data" refers to information stored in a database that can only be “consulted” via the “index”.

In view of the previous definition, and with regards to the data requirements for the new system (refer to section 4.1.1), the VIS will store the following types of information:

1. Alphanumeric Data;
2. Alphanumeric Index;
3. Photograph Data;
4. Biometric Data;
5. Biometric Index;
6. Supporting document Data;
7. Supporting document Index.

To simplify and facilitate ease of reading, the following table classifies the VIS data according to their intrinsic logical and physical nature.

Table 5-1: VIS data classification.

VIS data	Alphanumeric	Image
Alphanumeric data and index (1)	Alphanumeric data and indexes	Not applicable
Supporting documents and index	Document indexes	Supporting Documents image
Biometrics	Not applicable	Biometrics image and template[17]
Photograph	Not applicable (2)	Photograph image

(1) mainly application forms and visa stickers
(2) photograph indexes are not considered because searches are not foreseen in photographs

Henceforth, VIS will store *alphanumeric* and *imaged* data. *Alphanumeric data* by nature is low in volume and suitable for search purpose, whereas images are not convenient for searching. Images are consulted using unique keys, determined by a search operation on the alphanumeric data.

In the particular case of biometrics, the scanned imaged data (e.g. fingerprint images) are translated into templates, subsequently used for the search process. In the case of documents, the scanned documents are associated to indexes, which are alphanumeric and searchable.

With regards to Figure 5-1, different repartitions of the data are possible among the Central and the National systems. The choice of the system architecture (and thus the data repartition) largely depends on the size and nature of data stored and processed by the VIS, which is reported in Table 5-2. **Besides the alphanumeric data with size 6 Kbytes per visa record, all other data components are voluminous and consist mainly of digitised images.**

Table 5-2: VIS data record size.

Data Type	Record size (kbytes)	Total size (Tera bytes)
Alphanumeric	6	0.6
Photograph (image)	45	3.2
Biometric (image)	Fingerprints: 250 (ten fingers) Iris: 2 (one iris) Facial: 45	Fingerprints: 17 (ten fingers) Iris: 0.14 (one iris) Facial: 3.2
Supporting documents (image)	180	18

The total size is calculated on the basis of 20 Million visas, with a five (5) year retention period, which gives the total of 100 Million visa application records. Concerning the biometric images and photographs, a total reference figure of 70 million is used for calculating the total size, as a result of frequent travellers requesting a visa for a second time.

The VIS data will be accessed and processed by the VIS business processes as introduced in Chapter 2. These processes include *visa issue with/without previous registration, visa and traveller verification* and *person identification*.

VIS data and business processes could be stored and accessed at the Central level, National level or at both. This is examined below when some generic solutions for the VIS architecture are considered.

[17] A template is the digital equivalent (e.g. 010110) of a biometric image suitable for search operations.

5.3.2 Generic solutions

The section examines three generic solutions for the data and function repartition and determines the impact of each solution. **The drawn conclusions determine the two candidate solutions for the architecture of the VIS.**

With regard to Figure 5-1, the data, indexes and the system functions can be stored at the Central level or at National level or at both (Central and National):

1. The configuration where data and functions are exclusively stored at Central level is referred to as the "*Central solution*";

2. The configuration where data and functions are exclusively stored at National level is referred to as the "*Distributed solution*";

3. The configuration where data and functions are stored at both the Central and the National level is referred to as the "*Replicated solution*".

The "*Central solution*" is the simplest of the three. It consists of a single database (without data replication or distribution), and a single application environment located at the Central location. Access to the data and functions are performed on the central system.

The "*Distributed solution*" is more complex than the "*Central solution*". Data and functions are stored at national level. The role of the central system is to facilitate the distributed communication between the national systems. As we shall see, distribution of fat data at national level lowers the communication requirements but results in complex search and consultation processes.

The "*Replicated solution*" is the most complex of them all, as all data stored in the Central system is replicated on the National systems. Therefore, data and the functions are stored at national level. Replicating information at national level, improves the search and consultation process, but makes it more difficult to carry out any insert/update processes.

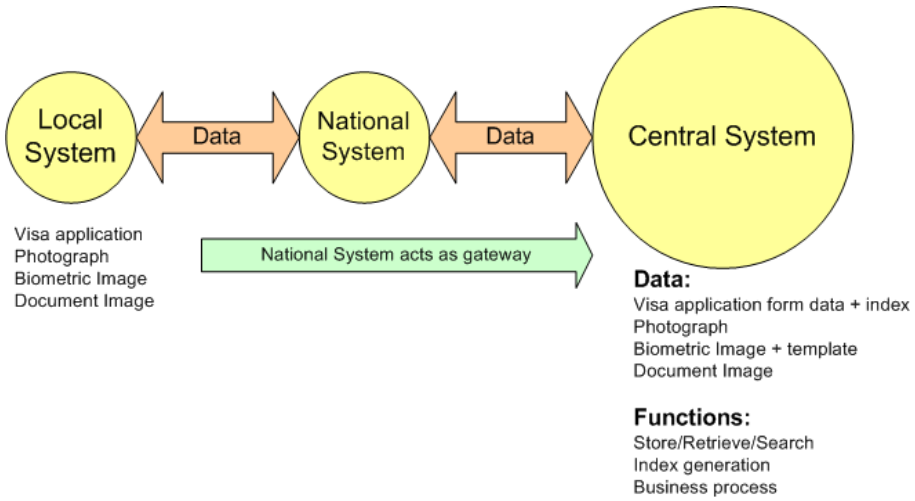
Various combinations of the above solutions are possible depending on the type of data and the business context. For instance, it is possible to centralise the biometric index (allowing for an efficient search), replicate the alphanumeric index (allowing for faster search/consultation response time) and distribute the photographs (reducing network bandwidth usage).

These have been examined below with a view to identifying **at least one and preferably several technically feasible solutions for the VIS architecture**.

5.3.3 Centralised solution

Figure 5-3 illustrates the architecture for the centralised solution. In this configuration, data and the business logic (functionality) is centralised and national systems act as simple gateways to provide access to the services supported by the VIS. Local systems (consulates) and their end-users are connected to the VIS services via their respective national systems.

Figure 5-3: Centralised solution.



Typical information flows in this configuration are:

1. **Insert** - this process concerns the introduction of new information into the system (e.g. a new visa), as well as updating existing data. Information (visa application form, photograph, biometric image, document image) is collected, digitised and subsequently transmitted via the **national system** to **the central system** for storage and processing;

2. **Search** - this process concerns multiple criteria searches performed by the users of the local systems to find possible matches. Users, at local level, query (e.g. for applicant name) the central system to identify possible matches (e.g. previous registered person);

3. **Consultation** - this process concerns direct access to specific information stored in the central system. Users, at local level, using unique keys (e.g. a visa sticker number) consult the central system in order to retrieve the appropriate data (e.g. complete sticker information).

Advantages/disadvantages:

1. Easier to administrate the system development and implementation cycles, reducing financial and human resources burden;

2. Easy to administer and maintain a single *"complex/fat"* central system;

3. Easy to introduce new Member States to the VIS;

4. Communication infrastructure costs are high due to centralisation of voluminous data, (document, photographs and biometric images);

5. The cost of business continuity system is high but applied to a single location (the central system);

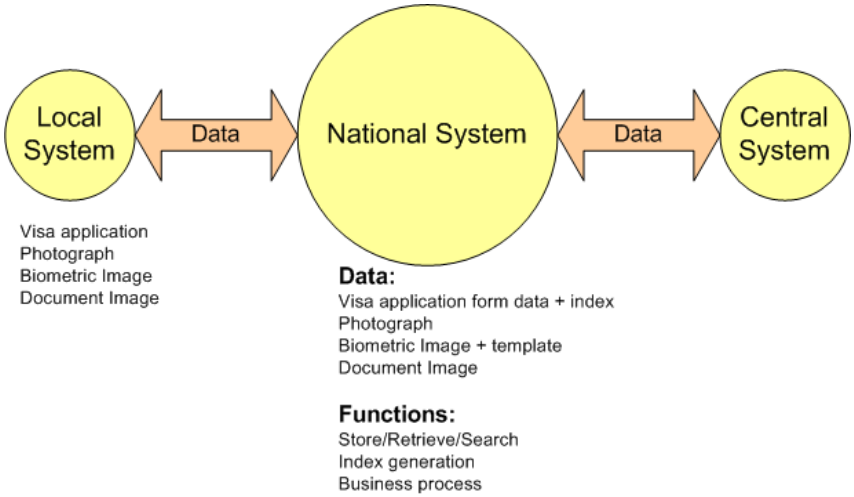
6. Strong dependency on a central system to support the VIS business context. This should be balanced with the availability of a business continuity planning;

7. Performance could become a problem as data and processes reside at a single *"fat"* location/system.

5.3.4 Distributed solution

Figure 5-4 illustrates the architecture of the distributed solution. In this configuration, data and most business logic are decentralised at the national level with only a few business logic at the central level. **The difference with regards to the centralised solution is that here we deal with more sophisticated architectures at National level, reducing the complexity of the central system.**

Figure 5-4: Distributed solution.



Typical information flows in this configuration:

1. **Insert** – Information collected at local level is subsequently **transmitted and stored at National level**;

2. **Search** – Users at local level, query the national systems, which subsequently query **all the other (27 in total) national systems** to find a possible match. The central system supports the distributed communication management between the national systems;

3. **Consultation** - Users at local level, using unique keys (e.g. a visa sticker number) consult the national system to retrieve the appropriate data (e.g. complete sticker information). Consultation involves **a number of national systems**.

Advantages/disadvantages:

1. Global Storage requirement equivalent to centralised solution, but this time, is distributed over N (N=27) locations;

2. Search process is very complex and requires large processing power and bandwidth. This architecture is suited to systems that manage certain categories of data that are 'not searchable', like images (e.g. photographs, biometrics images, supporting document images);

3. Consultation process is simple and efficient only if information is exclusively stored at national level. Where visa information is distributed among several Member States, the complexity of the consultation process increases significantly;

4. Reduces the communication infrastructure requirement at central level (as voluminous data is decentralised at national systems);

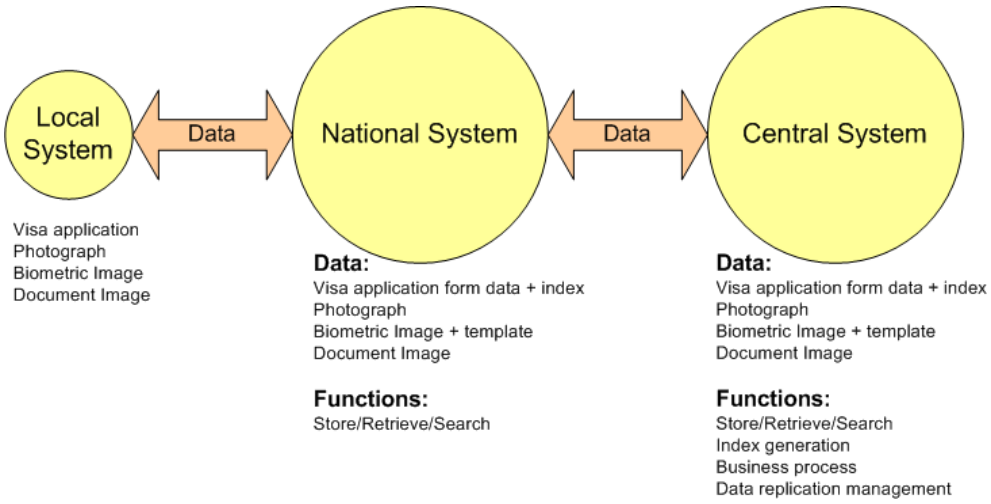
5. Administration and maintenance complexity increases, having to deal with a large number of complex systems, one per Member State;

6. Business continuity planning is more complex, having to deal with N national systems compared to a single central system in the previous solution.

5.3.5 Replicated solution

Figure 5-5 illustrates the architecture of the replicated solution. In this configuration data and business logic resides at National as well as at Central level. Note the difference with regards to the centralised and distributed architecture. Here **we deal with sophisticated systems architecture at both the National level and Central level, increasing the overall complexity of the system**.

Figure 5-5: Replicated architecture.



Typical information flows in this configuration:

1. **Insert** - Information is collected and subsequently transmitted via the national system to the central system for storage and processing. The central system mirrors the data to all the national systems (27 in total);

2. **Search** – The entire data set is stored at national level, thus information queries execute directly at national level without any interaction with the central system;

3. **Consultation** – Consultations are performed against data stored at national level without any interaction with the central system.

Advantages/disadvantages:

1. The complexity of the national systems increases significantly, having to deal with fully sized systems, one per Member State, in addition to the central one. This translates into increased costs for hardware and software, the biometric infrastructure, business continuity systems;

2. Data storage requirements increase dramatically (N+1 complete storage) as the complete set of data is stored at national level. This has a significant impact on the investment costs;

3. The mirroring of data from the central to the national systems requires large bandwidths, which has a significant impact on the communication costs;

4. Search and consultation processes are executed at national level, providing optimum response times compared to the previous two solutions;

5. Insert process is very complex, requiring high bandwidth and processing power as data is replicated from the central to the national systems;

6. Administration and maintenance complexity increases, because of the large number of systems. This has a dramatic impact on the human resources costs;

7. Business continuity could be introduced, as one national system could serve as the fail-over of another. However the communication management complexities for data replication between national systems makes this option complex and almost unmanageable.

5.3.6 Assessment of the solutions

Table 5-3 compares the three solutions against a comprehensive set of selection criteria so as to determine their suitability to the VIS context.

Table 5-3: Assessment of the generic solutions.

Selection criteria	Central	Replicated	Distributed
Data Storage Requirements	1*DSR	(1 + N) * DSR	1 * DSR (distributed over N locations)
Processing Requirements	Low	Medium	High
System Administration	Normal	Complex	Average
System Maintenance	Normal	Complex	Average
Communication Requirements	High	Very High	Moderate
Business Continuity	Normal	Complex	Complex
Total Cost of Ownership	High	Very High	High
Development Complexity	Normal	Complex	Complex
Response Time	Average	Good	Poor
Overall Complexity	**Complex**	**Impractical**	**Very complex**

DSR = Data storage capacity requirement
N = number of National systems which in the VIS case equals to the 27, and includes the current Member States and the ones in Accession plus Iceland and Norway.

With regard to the previous table, the **replicated solution is considered impractical and not suitable for the VIS architecture** due to:

1. The global data storage requirements that are very high compared to the other solutions (**27 times more, compared to a centralised or replicated solutions)**;

2. The complexities associated with the system administration and maintenance procedures, for example having to **manage and maintain 27 "fat" sites instead of one (1) for a centralised solution**;

3. Very high communication infrastructure requirements **to replicate voluminous data (e.g. photo, biometric images) from the central system to 27 "fat" national sites**.

The large number of shortcomings associated with the replicated solution outperforms its sole benefit, which is the optimum response time. **Therefore the replicated solution should not be further considered in the context of VIS.**

In view of this, we can conclude that only the Centralised and the Distributed solution are suitable for the VIS.

5.3.7 Conclusion of the Generic Architectures

Taking into consideration the storage, processing and communication requirements for each type of data stored and processed by the new system, Table 5-4 determines **the two solutions for the VIS architecture**.

Table 5-4: Architectural solutions for VIS (data perspective).

VIS data types	Central	Distributed
Alphanumeric data	Optimum	Not recommended
Alphanumeric index	Optimum	Not recommended
Document index	Optimum	Not recommended
Document image	Possible	Optimum
Biometrics templates	Optimum	Not recommended
Biometric images	Possible	Optimum
Photograph images	Possible	Optimum

Taking on board the previous table, the two solutions for the architecture of the VIS are as follows:

1. A purely ***centralised solution*** **where all the data (images and alphanumeric) is stored at a central system**. The solution provides simplicity for development and implementation, as well as administration and maintenance;

2. A ***hybrid*** **solution which is a combination of the Central and Distributed as indicated by the grey boxes on the above table.** In this solution the **"voluminous images" data is stored at national systems (thus distributed) whereas "alphanumeric" data and biometric templates are stored at central systems (centralised)**. This is an alternative to the previous solution in view to reduced telecommunication costs at the expense of increasing the complexities due to voluminous data decentralisation.

The above are the two solutions that will be considered for the VIS. Prior to introducing them, the following section will discuss the similarities between VIS and SIS II.

5.4 DEFINITION OF THE VARIOUS VIS COMPONENTS

Having regard to the Council guidelines, the structure of the VIS must be similar to that of the existing Schengen Information System (SIS). In view of this, Figure 5-6 illustrates a high level representation for the VIS architecture comprising of:

1. A **C**entral Visa Information **S**ystem (C-VIS);

2. The **N**ational Visa Information **S**ystem (N-VIS), the VIS notation component exposing the VIS functionalities at national level;

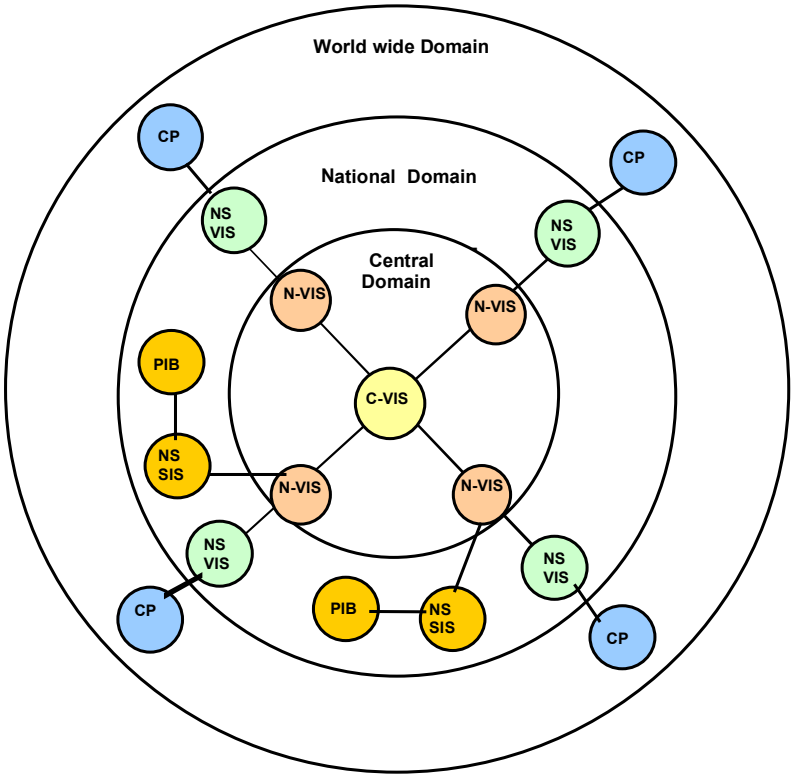
3. The world-wide diplomatic consular posts (CP) connected to National Systems (NS VIS) and to the VIS.

With regards to this novel architecture for the VIS system:

1. Existing National Visa Systems (NS VIS) operated by the Member States (connecting the diplomatic missions and consular posts) connect to the VIS at the N-VIS level;

2. Member States authorities and existing National systems must connect to the N-VIS to benefit from the VIS services. This is the case for **p**olice, **i**mmigration and **b**order checkpoints (**PIB**), connecting to the N-VIS via the SIS infrastructure.

Figure 5-6: The VIS architecture.



Legend:
CP refers to **C**onsular **P**ost
NS-VIS refers to **existing national visa systems** operated by the Member States
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)
NS-SIS refers to the existing Schengen infrastructure (SIS II)
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities.

In conformance with the SIS architecture, the VIS system comprises a Central Information System (C-VIS) and a National Visa Information System (N-VIS), in each Member State. N-VIS is the national gateway to the VIS services.

At a high level, two options are applicable with regards to connecting to the VIS:

1. **Member States with existing national visa systems (NS VIS) connecting their consulates, should consider connecting these existing systems to the N-VIS to make use of the VIS services;**

2. **Member States that do not operate national visa systems could consider connecting their world-wide consular posts directly to the National Visa Information System (N-VIS). <u>This latter case shall only be considered here when examining Option 1, which deals with the separate solution for the VIS.</u>**

There are some typical examples:

Consular Posts are connected to the Ministry of Foreign Affairs. Connecting the Foreign Affairs systems to the N-VIS, will facilitate access to the VIS services with a view to support the visa issue and visa consultation procedures performed by the consulates.

A Member State does not operate a national system that connects to its world-wide consular posts. In this case, the Member State could consider establishing the National Visa Information System (N-VIS) at the Foreign Affairs Ministry (or in another competent Ministry) and connect its consular posts directly to the VIS.

Likewise border checkpoints, police and immigration authorities could connect their national systems (NS of the SIS) to the N-VIS to access the VIS verification and identification functionalities.

The responsibility for connecting national authorities of the Member States to the N-VIS is delegated to the Member States. The Community will ensure that the VIS services are operational at National level (N-VIS).

The table illustrates the corresponding elements of the VIS and SIS II components.

Table 5-5: Elements of VIS and SIS II components.

SIS component	VIS component
CS – Core System	C-VIS (**C**entral **V**isa **I**nformation **S**ystem)
NI – National Interface	N-VIS (**N**ational **V**isa **I**nformation **S**ystem)
NS – National Systems	NS – National Systems connecting: Consular posts/diplomatic missions Border checkpoint authorities Police authorities Immigration authorities

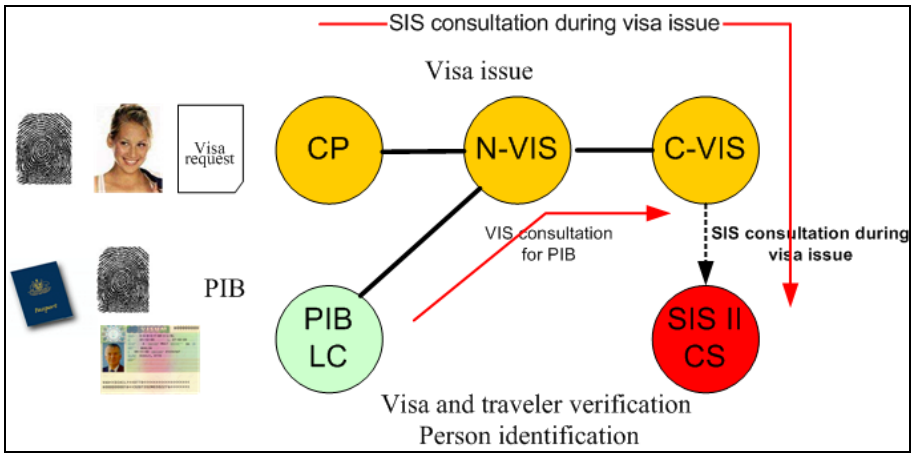
Having established the architectural similarities between the SIS II and the VIS, the following examines the solutions **for a separate VIS system** (Option 1) and subsequently develops the case for applying synergies through the **technical integration between the VIS and SIS II** (Option 2).

5.5 OPTION 1: SEPARATE SOLUTION FOR VIS

Figure 5-7 illustrates a high level architecture for the VIS as a separate system with regards to the SIS II. By maintaining the separation between the systems, it introduces the procedures associated with the two core information flows of *visa issue* (top part), *visa and traveller verification* and *person identification* (lower part).

It should be noted that the *visa issue, person identification* and *visa and traveller verification* is performed via the VIS infrastructure.

Figure 5-7: High level view of the separate VIS and SIS II.



Legend:
CP refers to **C**onsular **P**ost
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities which could possibly be the **NI** of the SIS II
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
SIS II CS refers to the core system of the SIS II.

With regards to *visa issue*, travellers lodge visa requests with the consular posts (CP) of the Member States. The uniform visa applications, the photograph, the biometric information and supporting documents are acquired and digitised. The compound visa data "dossier" is prepared, registered in the VIS and subsequently transmitted to the national (N-VIS) and the central (C-VIS) system for storage and processing. Upon registration, the consultation process with the national central authorities is initiated in order to assess and make decision on the visa application. The visa issue decision (whether taken by the consular post or by the national central authority) is electronically registered in the VIS systems including the grounds for that decision and subsequently transmitted back to the consular post in charge of delivering the visa sticker (in the case that a visa is granted). The visa issue information flow will automatically trigger the consultation with the SIS II (indicated as SIS consultation during visa issue) in order to verify whether an alert has been issued on the applicant in the SIS II for the purpose of refusing entry. Moreover, although not indicated in the figure, the VIS will implement the VISION consultation should the applicant come under the categories listed in Annex 5B of the Common Consular Instructions.

Border checkpoint authorities in charge of *visa and traveller verification* connect their local systems to the N-VIS infrastructure. This will facilitate these authorities' access to the VIS consultation functionalities in order to determine the authenticity of the sticker, verify the identity of traveller and to safely determine that the carrier is indeed the holder. Moreover the SIS II consultation is performed through the VIS to verify whether an alert has been issued on the traveller and to determine instances of counterfeited or stolen passports or visa stickers.

Likewise police and immigration authorities perform *person identifications* by connecting their local configurations to the N-VIS to determine a possible identity for undocumented persons or illegal immigrants.

Note: Connecting the local configuration of the police, immigration and border checkpoint authorities to the N-VIS facilitates the exposure of *verification* and *identification* services to these authorities. **The network connecting the PIB authorities to the N-VIS is not currently available. Member States should consider connecting thousands of police and immigration local configurations (or the central systems connecting the local configurations) to the N-VIS.**

The following sub-section will deal with the two specific solutions for the architecture of the VIS, the *centralised* and *hybrid* determining the technical and operational requirements for each of them. These requirements are translated in chapter 7 to illustrate their impact in financial, human and physical resources.

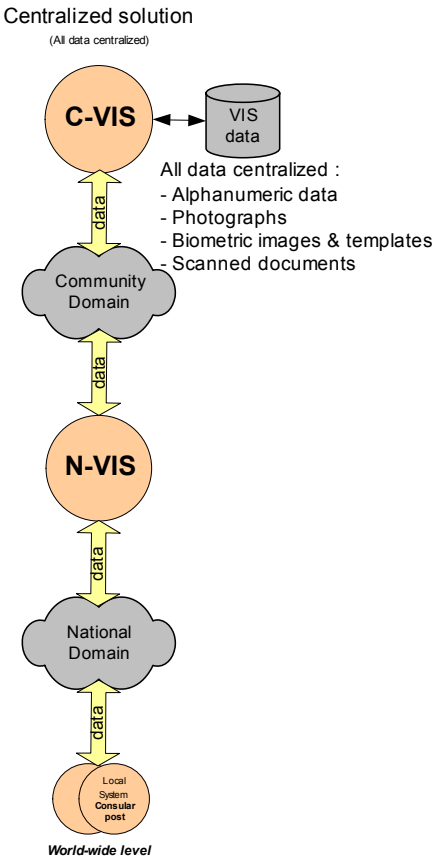
5.5.1 Option 1, Solution 1: Centralised Solution for the VIS

This solution refers to the second column of Table 5-4, noted as "Centralised", where **all the visa data and system functions** are stored at and managed by the Central System (C-VIS).

5.5.1.1 Description of the architecture

Figure 5-8 illustrates the centralised solution for the architecture of the VIS. It is characterised by a *"fat and complex"* central data storage and processing facility (the C-VIS), and *"low complexity"* national system (N-VIS) that operates as a simple gateway for the national users.

Figure 5-8: Centralised architecture for the VIS[18].



From an operational perspective in this architecture:

1. Data (alphanumeric data, photographs, biometrics and supported documents) acquired by the consular post officials during the visa issue procedure is digitised and transmitted to the National System (N-VIS). N-VIS operates as a communication hub with reinforced security, relaying all the national traffic to the central storage and processing facility (C-VIS);

2. Consultation requests submitted by the consular posts, and other national authorities (police, immigration services, and existing national visa system) are routed to the N-VIS system via the national domain. Subsequently these requests are transmitted through the community domain to the central C-VIS system for execution (refer to Figure 5-7).

From a technical perspective:

1. Data is stored at the central system C-VIS in appropriately dimensioned databases, each fine-tuned to process a specific type of data. Indexes are generated to facilitate the consultation operations. Alphanumeric data and in particular names, surnames and other personal peculiarities are transliterated into the various languages to facilitate searches in multiple languages. In addition, the biometric images are translated to templates to be subsequently used for biometric matching operations during the verification and identification procedures;

[18] Network architecture is explained in Chapter 6.

2. To provide high availability and business continuity, data stored in the C-VIS is automatically mirrored to a fail-over system at a different physical location. This fail-over location is sized so as to support the full VIS operations in the event of a failure of the production C-VIS site.

The following examines the technical impact of the centralised solution and provides a direct comparison with the hybrid solution introduced later on in section 5.5.2.

5.5.1.2 Impact on data storage, functionality, communication and technical infrastructure

Table 5-6 introduces the technical impact of the centralised architecture for the C-VIS and N-VIS taking into consideration the types of data to be stored in the system. The reported figures are based on 20 million visa requests per year and assume a five (5) year retention period, leading to 100 million visa application records. For biometric images and photographs a figure of 70 million is used to calculate the volumes as a result of frequent travellers requesting visa for a second time. In the table one can find the impact of the two response time scenarios introduced in Chapter 4.

Table 5-6: Impact of the centralised solution for the VIS.

	C-VIS		N-VIS	
Alphanumeric data				
Data Storage Requirement	600 GB		0	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps)	0.384	0.384	CAT 3: 0.064 CAT 2: 0.064 CAT 1: 0.064	CAT 3: 0.064 CAT 2: 0.064 CAT 1: 0.064
Main Functionality	Storage Multi-criteria search Retrieve Transliteration Phonetic + truncated equivalent		None	
Special Hardware	Database server Application server		None	
Photo				
Data Storage Requirement	3,200 GB		0	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	13.000	13.000	CAT 3: 1.536 CAT 2: 0.384 CAT 1: 0.384	CAT 3: 3.000 CAT 2: 3.000 CAT 1: 3.000
Main Functionality	Storage Retrieve		None	
Special Hardware	Image server		None	
Biometrics				
Data Storage Requirement (ten fingers)	175 GB for templates 17,000 GB for images		0	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	21.100	21.100	CAT 3: 1.536 CAT 2: 0.448 CAT 1: 0.448	CAT 3: 3.200 CAT 2: 3.200 CAT 1: 3.200
Main Functionality	Template extraction Storage Identification Verification		None	
Special Hardware	Biometric matching engine		None	

	C-VIS		N-VIS	
	Image Server			
Documents				
Data Storage Requirement	18,000 GB for images		0	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	25.700	25.700	CAT 3: 1.664 CAT 2: 0.448 CAT 1: 0.448	CAT 3: 3.200 CAT 2: 3.200 CAT 1: 3.200
Main Functionality	Storage Search Retrieve		None	
Special Hardware	Database server Image server		None	

5.5.1.3 Impact on business information flows

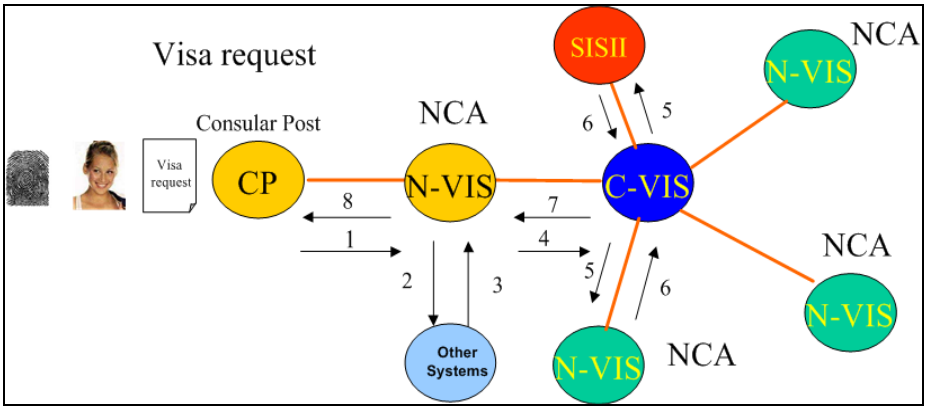
The following discusses the impact of the centralised solution on the VIS information flows, in particular the *visa issue, with and without previous visa registration*, *visa and traveller verification* and *person identification*.

Visa issue (refer to Figure 5-9): Consular posts (CP) acquire the visa data from a new visa applicant, prepare the compound visa data "dossier", which is subsequently transmitted to the national (N-VIS) for processing by their competent national central authorities (1). The new visa application can be checked (executed) against data stored in the national visa information systems operated by the Member States (2) in order to make a visa issue decision (3). The "dossier" with the full set of applicant's data is subsequently forwarded from the N-VIS to the central system (C-VIS) for storage and processing (4). An essential part of the processing is the extraction of the biometric data, and the execution either of an identification procedure *for new applicants without previous registration* to the VIS, or a verification *for visa applicants with a previous visa registration*.

Once the visa data "dossier" is registered in the central system, the SIS II consultation is automatically initiated to determine whether an alert has been issued on the applicant in the SIS (5,6).

The VISION functionality, integrated into the VIS, is initiated by the central systems (C-VIS) which will communicate this new visa registration to the N-VIS of one or more Member States (5,6). The combined result of SIS and VISION consultation (two requests launched in parallel), the VIS verification or identification are transmitted back to the consular post (7,8) via the N-VIS, to make an informed decision to be made on the issuing of the requested visa. In the information flow, all data is centralised at the C-VIS, **therefore the complete visa history of a traveller is centrally stored and administered, and future retrieval operations will be easier to administrate.**

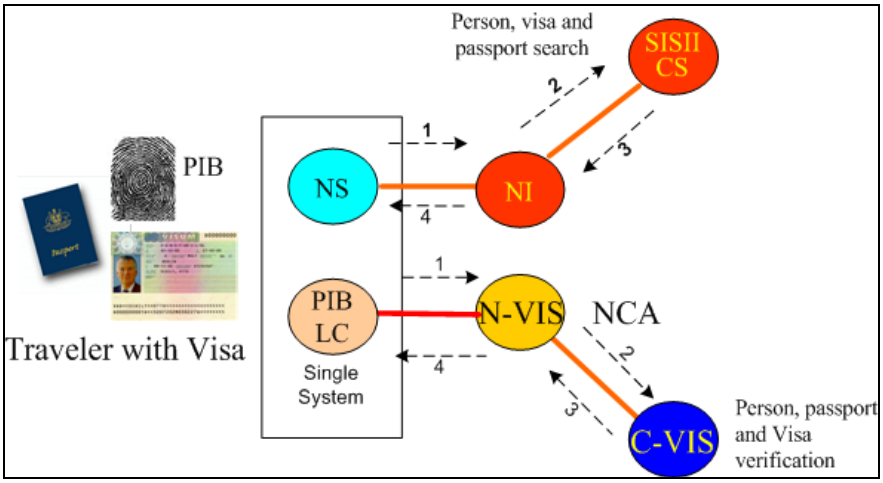
Figure 5-9: Visa issue.



Legend:
CP refers to **C**onsular **P**ost
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystems (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)
SIS II refers to the SIS II
Other systems refer to existing national systems operated by the Member States.

Visa and traveller verification (refer to Figure 5-10): Border checkpoints check the passports and visa sticker and acquire biometrics from the travellers. The captured data is transmitted through the SIS infrastructure from the NS to the NI (1) and the SIS search (2) is initiated at the CS to determine whether an alert has been issued on the traveller in the SIS (3,4). Likewise, the border checkpoint authorities through the local configuration connected to the N-VIS (1) execute the traveller verification request at the C-VIS, (2,3). The combined results of the SIS II search and VIS verification will be subsequently transmitted to the end-user.

Figure 5-10: Visa and traveller verification.

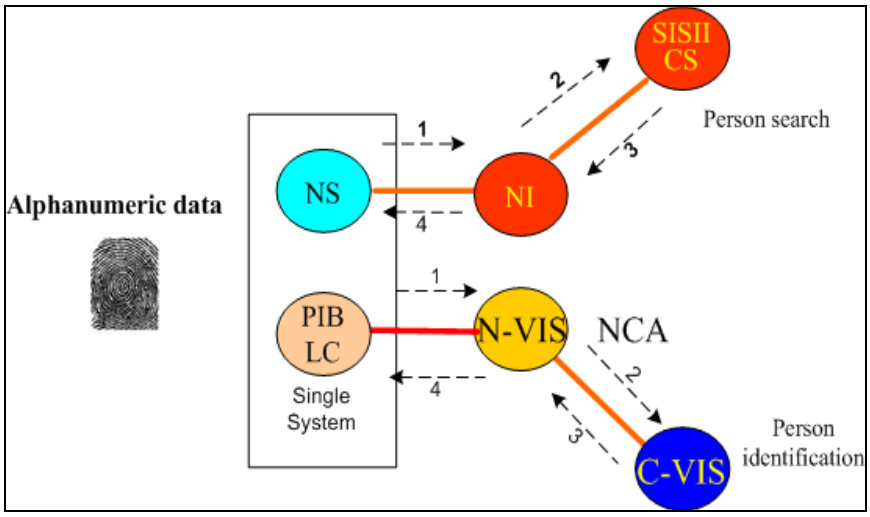


Legend:
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities
NS refers to the National System of the Schengen infrastructure (SIS II)
NI refers to the **N**ational **i**nterface of the SIS II
SIS II CS refers to the core system of the SIS II
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)

Person identification (refer to Figure 5-11): The information flow is identical, the difference being that we mainly deal with undocumented persons intercepted at police or immigration checkpoints. VIS and SIS II are simultaneously consulted to determine a possible identity. In

particular, the VIS services are exposed to the PIB authorities solely via the N-VIS, therefore these authorities need to connect their local configurations to the N-VIS.

Figure 5-11: Person Identification.



Legend:
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities
NS refers to the National System of the Schengen infrastructure (SIS II)
NI refers to the **N**ational **i**nterface of the SIS II
SIS II CS refers to the core system of the SIS II
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)

5.5.1.4 Communication requirements

Table 5-7 illustrates the communication requirements of the centralised solution, displayed separately for the C-VIS and the three categories of N-VIS as well as for the two response time scenarios defined in chapter 4. Note that the figures are cumulative starting from the alphanumeric configuration, photographs, biometrics and lastly the supporting documents.

Table 5-7: Required bandwidths cumulative (Mbps) for the Trans-national Domain.

Location	Alphanumeric data	+photographs	+biometrics	+documents
Centralised architecture - Response time T_1				
C-VIS	0.384	13.000	21.100	25.700
N-VIS cat. III	0.064	1.536	1.536	1.664
N-VIS cat. II	0.064	0.384	0.448	0.448
N-VIS cat. I	0.064	0.384	0.448	0.448

Location	Alphanumeric data	+photographs	+biometrics	+documents
Centralised architecture - Response time T_2				
C-VIS	0.384	13.000	21.100	25.700
N-VIS cat. III	0.064	3.000	3.200	3.200
N-VIS cat. II	0.064	3.000	3.200	3.200
N-VIS cat. I	0.064	3.000	3.200	3.200

The network requirement at central level C-VIS level is very high (25.7 Mbps). The following presents an alternative solution (hybrid solution) to examine how the communication infrastructure requirement and therefore telecommunication costs could be reduced.

5.5.1.5 Security responsibility

Security aspects specific to the solution:

N-VIS will act only as a communication point. Physical **on-site** intervention on the N-VIS site will not be very frequent. The protection requirements in terms of **physical** access controls are very limited for the N-VIS in the central solution.

Although, the C-VIS site needs a larger storage capacity (biometrics and document images) and a larger communication capacity between the N-VIS sites to transmit these images, these additional requirements only add a marginal complexity to the security plan. In the central solution, normally more personnel would work on the C-VIS site. However this does not really influence the complexity of the access control for the sites. Indeed, in the 2 solutions C-VIS must implement an extremely highly secured environment, especially for access control.

Business continuity assessment:

A failure in the N-VIS of a Member state implies a corresponding discontinuity of the visa business for that Member State.

The failure of one, several or all the functions of the C-VIS imply a corresponding discontinuity of the visa business for all Member States.

The **C-VIS** should be considered as the main point of vulnerability.

How does the solution meet business continuity?

As each N-VIS is only working as a communication point, each N-VIS site needs only to preserve its capacity to communicate with its national systems and the C-VIS. Thus business continuity planning is simpler at national level, N-VIS.

Fatter main and back-up C-VIS systems are required to assure business continuity. This has an influence on the amount of hardware for the C-VIS and its back-up site. But, this redundancy does not have an impact on the complexity of the security procedures (systems administrations, access control, and the contingency procedures).

What are the measures and how are these measures implemented in the context of the solution?

For the C-VIS, there is no real specific measure versus the other solution.

For each N-VIS, the Contingency plan is limited to the (higher) communication capacity.

5.5.1.6 Conclusions

The major drawback of the central solution relates to the high telecommunication infrastructure costs as a result of centralising the visa data from the world-wide consular posts of the Member States. This is reflected in the high telecommunication costs in the expenditure table.

This drawback should be weighted against the numerous benefits introduced by the solution, which are:

1. Easier to deploy a single centralised system and data centre to support the decentralised *visa issue* and *visa control* procedures of the Member States;

2. Project management risk is reduced having to set-up a single "complex" central systems compared to many "medium complexity" distributed systems, as is the case in the hybrid solution;

3. Easy to administer and manage a single "complex" system (e.g. several systems with a single data centre) compared to a large number of "medium complexity" systems (27 systems and data centres). Easier to administer system scalability at the central systems (C-VIS), compared to 27 systems (hybrid solution);

4. Simpler to set-up and maintain a centralised business continuity system to support the VIS operations in the event of a failure in the production site, C-VIS;

5. Systems maintenance procedures are localised at a single central site, the C-VIS;

6. Easier to administer the security measures and policy at the central site, the C-VIS.

Table 5-8 provides the SWOT (**S**trengths, **W**eaknesses, **O**pportunities and **T**hreats) analysis of the central solution.

Table 5-8: SWOT Analysis (central solution).

Strengths	Weaknesses
– System development and deployment time is shorter (optimised). – System administration and management burden is localised at the central system, C-VIS. – Maintenance procedures localised at the central system, C-VIS. – Easier to set-up and administer a single business continuity system at central level, C-VIS. – Easier to administer the security measures and controls at the central system, C-VIS. – Easier to administer the system scalability and extensibility. – Reduced project management, strategic and financial risk due to technical and human resources centralisation.	– Increased network costs as a result of data centralisation and increased network traffic. – Complex central system configuration management (data servers, data centre, applications). – Single point of failure at the central system, C-VIS (but mitigated by the mandatory contingency plan).
Opportunities	**Threats**
– Easier to introduce new Member States. – Change management procedures easier to administer and to implement in a centralised architecture.	– Design, implementation and testing of the contingency planning are critical.

5.5.2 Option 1, Solution 2: Hybrid Solution for the VIS

For a data distribution perspective, this solution corresponds to the grey cells of Table 5-9. Low volume data as alphanumeric and biometric templates are stored on the Central System (C-VIS), whereas voluminous data such as photographs, biometric images and scanned documents are stored and managed by the National System (N-VIS).

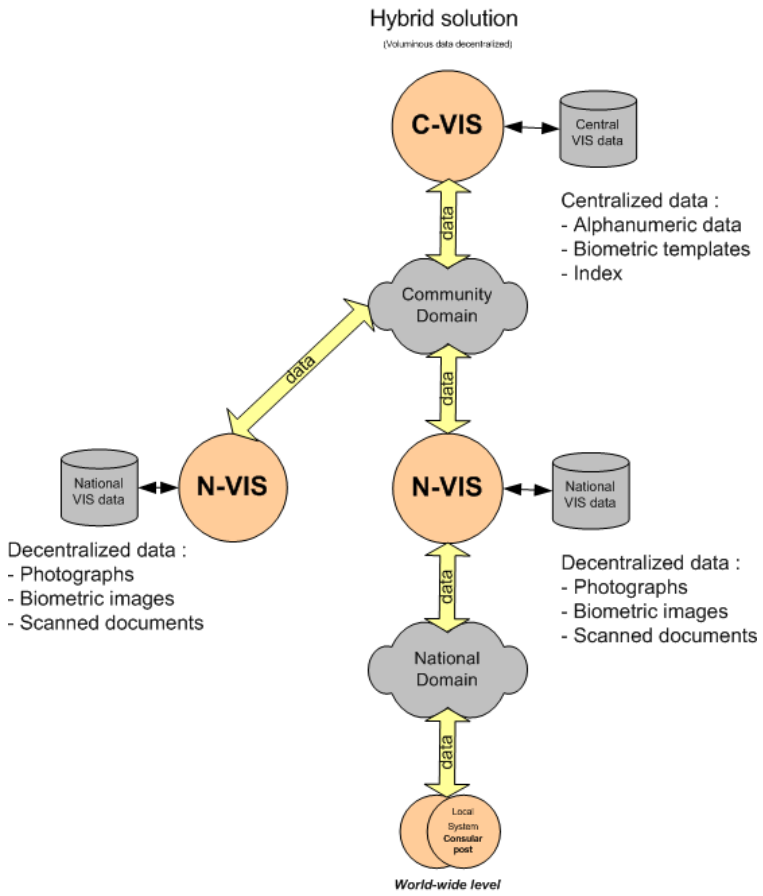
Table 5-9: Hybrid solutions for VIS (data perspective).

VIS data types	Central	Distributed
Alphanumeric data	Optimum	
Alphanumeric index	Optimum	
Photograph images		Optimum
Biometrics templates	Optimum	
Biometric images		Optimum
Document index	Optimum	
Document image		Optimum

5.5.2.1 Description of the architecture

Figure 5-12 illustrates the solution for the VIS architecture. It is characterised by a *"medium complexity"* central data storage and processing facility (the C-VIS) and *"high complexity"* national data storage and processing facility (N-VIS).

Figure 5-12: Hybrid VIS solution.



From an operational perspective:

1. Consular posts transmit the visa data through a secured network to their national N-VIS system. The local databases (N-VIS) are updated with the voluminous data, whereas alphanumeric data and biometric templates are subsequently transmitted to the central C-VIS system for further storage and processing;

2. Consultation requests submitted by a consular post are processed by their national system (N-VIS). If the data resides at a remote national system, the query is communicated to the central system (C-VIS) which relays it to remote national systems (N-VIS) where the data can be retrieved. This national system gathers information and transmits the combined results back to the requesting consular posts.

From a technical perspective, in this architecture:

1. Data is distributed between the C-VIS and the various N-VIS. Voluminous data such as photographs, biometric images and digitised supplementary documents are stored locally (at the N-VIS sites), while indexes and alphanumeric data is stored centrally (C-VIS);

2. The national N-VIS systems are more complex compared to the centralised solution (they host database and application servers) with routing functions to the central C-VIS system;

3. Supporting documents indexes are generated at national level (N-VIS) and subsequently transmitted for storage at the central systems C-VIS;

4. Similarly, the biometric images stored at national level N-VIS are translated to templates (at national level) and subsequently transmitted for storage to the central system, C-VIS to be used for biometric matching operations;

5. Alphanumeric data and indexes are stored and managed centrally. Moreover, alphanumeric data and in particular names, surnames and other personal peculiarities are transliterated into the various languages to facilitate search in multiple languages.

Therefore, having to store and process data at central (C-VIS) and at national (N-VIS) level increases the overall complexity of the architecture.

5.5.2.2 Impact on data storage, functionality, communication and technical infrastructure

Table 5-10 introduces the technical impact of the hybrid architecture for the C-VIS and N-VIS taking into consideration the types of data to be stored in the system.

Table 5-10: Impact of the hybrid solution for the VIS.

	C-VIS		N-VIS	
Alphanumeric data				
Data Storage Requirement	600 GB		0	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	0.384	0.384	CAT 3: 0.064 CAT 2: 0.064 CAT 1: 0.064	CAT 3: 0.064 CAT 2: 0.064 CAT 1: 0.064
Main Functionality	Storage Multi-criteria search Retrieve Transliteration Phonetic + truncated equivalent		Nothing	
Special hardware (indicative)	Database server Application server			
Photo				
Data Storage Requirement	0		CAT 3: 400 GB CAT 2: 80 GB	

	C-VIS		N-VIS	
			CAT 1: 16 GB	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	0.384	0.384	CAT 3: 1.4 CAT 2: 0.384 CAT 1: 0.384	CAT 3: 3.000 CAT 2: 3.000 CAT 1: 3.000
Main Functionality			Storage Retrieve	
Special Technical Equipments			Image server	
Biometrics				
Data Storage Requirement (ten fingers)	175 GB (for templates)		CAT 3: 210 GB (for images) CAT 2: 42 GB (for images) CAT 1: 9 GB (for images)	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	0.384	0.384	CAT 3: 2.432 CAT 2: 0.512 CAT 1: 0.384	CAT 3: 3.000 CAT 2: 3.000 CAT 1: 3.000
Functions	Storage Identification Verification		Template extraction Storage	
Special hardware (indicative)	Biometric matching engine		Image Server	
Documents				
Data Storage Requirement	100 GB for meta-data		CAT 3: 2,250 GB CAT 2: 450 GB CAT 1: 90 GB	
Response time	T_1	T_2	T_1	T_2
Communication Requirements (Community domain interface speed in Mbps - cumulated)	0.384	0.384	CAT 3: 3 CAT 2: 0.640 CAT 1: 0.384	CAT 3: 3.000 CAT 2: 3.000 CAT 1: 3.000
Main Functionality	Search Retrieve		Storage	
Special hardware (indicative)	Database server		Image server	

5.5.2.3 Impact on the business information flow

The following discusses the impact of the hybrid solution on the VIS information flows, in particular the *visa issue, with and without previous visa registration*, *visa and traveller verification* and *person identification* as well as the *retrieval of the visa history data* of a traveller.

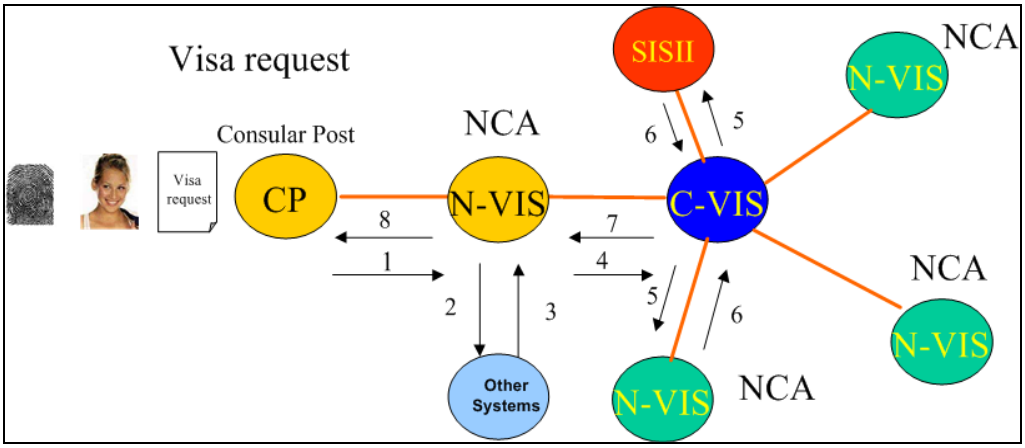
Visa issue (refer to Figure 5-13): Consular post (CP) acquire the visa data from a new visa applicant, prepare the compound visa data "dossier", which is subsequently transmitted to the national (N-VIS) for processing by their competent national central authorities (1). The new visa application is checked against data stored at the national visa information systems operated by the Member States (2) in order to make a visa issue decision (3). The image data (photograph, biometric images and supporting documents) is extracted from the dossier and stored locally at the N-VIS. The alphanumeric part of the dossier, including the computed biometric template and the supported document index is transmitted to the central system (C-VIS) for storage and processing (4).

Part of the processing at the central system is performing an identification procedure *for new applicants without previous registration* in the VIS, or verifying *for visa applicants with a previous visa registration*. The applicants computed template is extracted from the dossier, and the verification or identification process is initiated.

Once the visa data "dossier" is register at the central system C-VIS, the SIS II consultation is automatically initiated to determine whether an alert has been issued on the applicant in the SIS (5,6). The VISION functionality, integrated into the VIS, is initiated by the central systems (C-VIS) which will automatically communicate the new visa application to the N-VIS of one or more Member States (5,6). The combined result of the SIS and VISION consultation (two requests launched in parallel), the VIS verification or identification are transmitted back to the consular post (7,8) via the N-VIS, to allow a documented decision about the issuing of the requested visa.

In the information flow, as discussed later on, **the complete visa history of a traveller applying in different countries is distributed in a number of national systems, N-VIS. This introduces complexities when it comes to retrieving the visa history dossier of this particular traveller.**

Figure 5-13: Visa issuance (hybrid solution).



Legend:
CP refers to **C**onsular **P**ost
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystems (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)
SIS II refers to the SIS II
Other systems refer to existing national systems operated by the Member States.

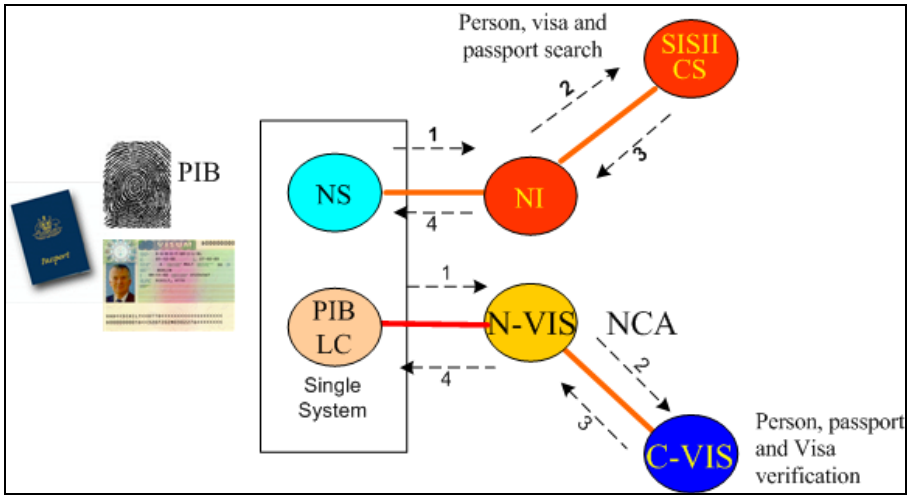
Visa and traveller verification (refer to Figure 5-14): Border checkpoints check the passports and visa sticker and acquire biometric from the travellers.

The captured data is transmitted through the SIS infrastructure from the NS to the NI (1) and the SIS search (2) is initiated at the CS to determine whether an alert has been issued on the traveller in the SIS (3,4).

Likewise the border checkpoint authorities, through the local configuration, connect to the N-VIS (1) and execute the traveller verification request at the C-VIS, (2,3). The combined results of the SIS II search and VIS verification will subsequently be transmitted to the end-user.

We can conclude that the visa and traveller verification process is identical to the central solution, as it is a process that is executed at the central system, C-VIS.

Figure 5-14: Visa and traveller verification.



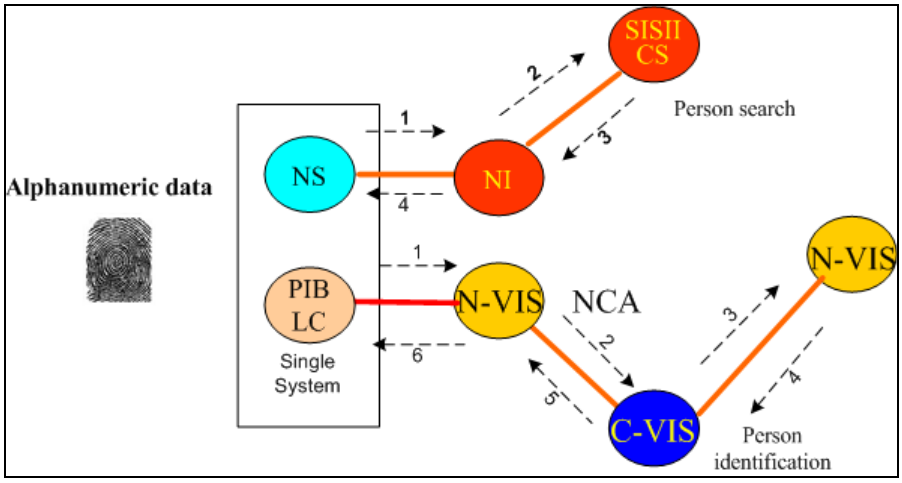
Legend:
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities
NS refers to the National System of the Schengen infrastructure (SIS II)
NI refers to the **N**ational **i**nterface of the SIS II
SIS II CS refers to the core system of the SIS II
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)

Person Identification (refer to Figure 5-15): The information flow is identical to the previous one except for one difference. Once the identification request is lodged, the biometric engine at the central level (C-VIS) will perform a one-to-many comparison to find a possible match. Due to the inaccuracy of biometrics (not 100%) **photographs are returned by the VIS system to the end users with a view to improving the accuracy of the identification.** In this particular case, screening will have to rely on the retrieval of the photograph and a comparison of the person with his/hers digital image stored in the VIS. As photographs are distributed across several national systems (N-VIS), the retrieval process introduces additional burden. **This burden should be carefully considered, as VIS will have to support 5 million identification requests.**

The retrieval of photographs has a significant impact on the bandwidth reported in Table 5-9. It has been assumed that one photograph is used in case of verification whilst ten of them are used in case of identification.

We can conclude that the person identification process is more complex, compared to the central solution, as photographs to assist the visual checks will have to be retrieved from other national systems, N-VISes.

Figure 5-15: Person Identification.

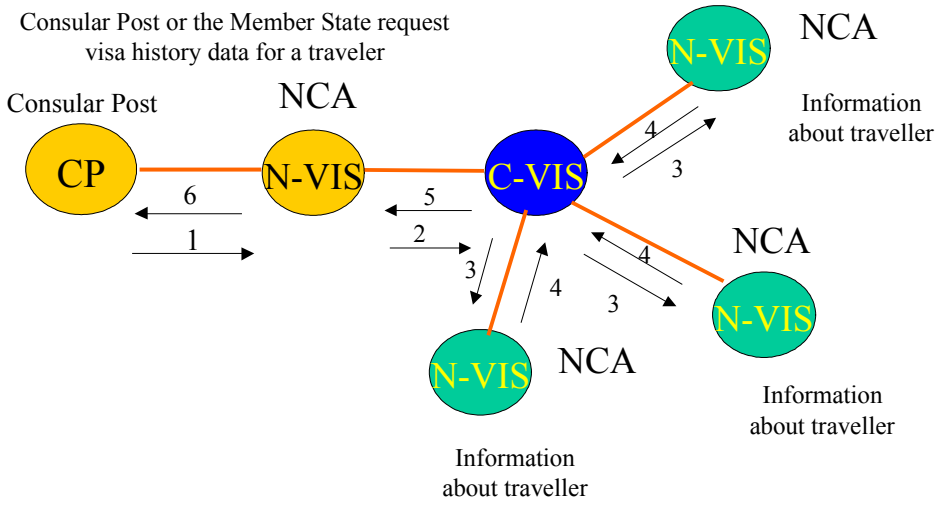


Legend:
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities
NS refers to the National System of the Schengen infrastructure (SIS II)
NI refers to the **N**ational **i**nterface of the SIS II
SIS II CS refers to the core system of the SIS II
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)

Dossier of the Visa history (refer to figure 5-16): The business impact of the hybrid solution is best determined in this new information flow. Consider the case in which a consular post or a national central authority lodges a request to retrieve the visa history dossier of a traveller who has **applied for visas in several countries over several years**. As a result of multiple visa requests in various countries, the "visa application history dossier" of the applicant is distributed in several National systems (N-VIS).

The consular post or the national central authority lodges the request to the N-VIS (1), which transmits the request to the C-VIS. **The C-VIS will find the corresponding indexes and locate where the data is located. Subsequently a data retrieval request will be communicated to the N-VISes. Data is retrieved and the visa history dossier of the applicant is composed** (including photographs and images of supporting document) (2,3). The visa history dossier is compiled at the C-VIS (from data received by the various National systems, N-VIS) and subsequently submitted back to the national central authority (or to the consular post) to aid the assessment of the particular visa request.

Figure 5-16: Visa consultation by NCA.



Legend:
CP refers to **C**onsular **P**ost
NCA refers to the **N**ational **C**entral **A**uthority
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)

As a result of the hybrid solution, the visa data (and in particular supporting documents) of a traveller is distributed over several national systems (N-VIS). Retrieving and compiling the full visa history "dossier" becomes a complex operation that involves retrieval from several national systems, N-VIS. **In view of this typical information flow, it could be considered that the solution is not optimum with regards to the process of a full visa dossier retrieval.**

5.5.2.4 Communication requirements

Table 5-11 illustrates the communication requirements of the hybrid solution.

Table 5-11: Required bandwidths cumulative (Mbps) for the Trans-national Domain.

Location	Alphanumeric data	+photographs	+biometrics	+documents
Hybrid architecture - Response time T_1				
C-VIS	0.384	0.384	0.384	0.384
N-VIS cat. III	0.064	1.400	2.400	3.000
N-VIS cat. II	0.064	0.384	0.512	0.640
N-VIS cat. I	0.064	0.384	0.384	0.384

Location	Alphanumeric data	+photographs	+biometrics	+documents
Hybrid architecture - Response time T_2				
C-VIS	0.384	0.384	0.384	0.384
N-VIS cat. III	0.064	3.000	3.000	3.000
N-VIS cat. II	0.064	3.000	3.000	3.000
N-VIS cat. I	0.064	3.000	3.000	3.000

Network bandwidth requirement is lower at C-VIS level, and a little bit higher at N-VIS level.

5.5.2.5 Security responsibility

Security aspects specific to the solution:

- N-VIS is a complex system, which comprises a data centre. It requires a very active and complex system administration, which has an impact on the human resources required (data administrators, system administrators, and specific technical equipment engineers). This implies a need to reinforce protection against attacks by IT insiders and a need to reinforce physical access control to installations;
- Although data is decentralised, the security controls at the central site cannot be any less than for the centralised solution.

Business continuity assessment:

- The failure of an N-VIS implies a corresponding discontinuity of the visa business for the Member State as well as of those that request retrievals of data from the national system where the discontinuity occurred;
- The failures of one, several or all the functions of the C-VIS imply a discontinuity of the visa business for the member states;
- The C-VIS does not store images (document and biometrics). The data storage requirements and the communication requirements are lower than in the centralised solution. Of course, this reduced requirement applies to the C-VIS back-up site capable of handling a complete disaster of the C-VIS site;
- In case of the failure of the C-VIS, it will still be theoretically possible for the member states to obtain the biometrics images and document images from the other national systems, N-VIS;
- Both the **C-VIS and N-VIS** should be considered as points of vulnerability.

How does the solution meet business continuity?

N-VIS in this solution consists of a complex system and data centre.

Thinner main and back-up C-VIS systems are required to assure business continuity. This has an influence on the investment costs to set-up the C-VIS and its back-up site. This does not have an actual impact on the administration of the security measures (systems administrations, access control) and contingency procedures.

What are the measures and how these measures are implemented in the context of the solution?

For the C-VIS there is no real specific security measure in comparison to the centralised solution.

For each N-VIS:

1. Complex contingency planning is required. In addition to acting as a communication point, each N-VIS locally stores document and biometrics images. This implies additional security requirements for the image servers for documents and biometrics. The handling of a complete disaster of an N-VIS is more complex. A comprehensive data replication solution is required between each N-VIS site and its back-up counterpart;

2. Internal security procedures of reinforcing protection against attacks by IT insiders;

3. Internal security procedures of reinforcing physical access control to installations.

5.5.2.6 Conclusions

The major drawbacks of the hybrid solution are:

1. Operational complexities increase as a result of having to manage and retrieve data, which is distributed in several (27) national systems (N-VIS) systems;

2. The increased complexity of the national systems (N-VIS) impacts on the financial and human resources required;

3. Difficult to manage the concurrent deployment of 27 national systems (N-VIS) and 27 data centres to supports the decentralised *visa issue* and *visa control* procedures of the Member States;

4. Project management risk increases, having to set-up a large number (27) of "medium complexity" national systems;

5. Systems administration and management burden increases because of the large number of distributed national systems, N-VIS in addition to the central system, C-VIS. Scalability management also becomes significantly more complex having to deal with 27 sites (N-VIS);

6. Systems maintenance (upgrades, updates) becomes much more complex having to deal with 27 decentralised systems, N-VIS in addition to the central system (C-VIS);

7. Business continuity planning becomes more complex as the N-VIS complexity increases. The set-up and administration of business continuity systems has an impact on investment and human resource costs. In general, business continuity planning is more complex having to deal with N back-up systems, one per Member State.

These drawbacks should be weighed against the benefits provided by the hybrid solution, which are mainly:

1. Reduced telecommunication costs as a result of storing "fat" imaged data at national level (N-VIS) rather than transmitting this data at the central system (C-VIS);

2. The operational efficiency associated with the *visa and traveller verification* process. A traveller applies for a visa in the consular posts of the Member State of its main destination. Storing the photographs and other "fat" imaged data at the National level (N-VIS) will facilitate the fast execution of the visa and traveller verifications procedure due to data being retrieved at National level rather than having to be retrieved from the centralised location (C-VIS).

   This advantage is no longer applicable if a decision is reached to use smart cards in the context of VIS to support *visa and traveller verification* at border checkpoints. The use of smart cards to support verification is discussed in chapter 3.

Table 5-12 provides the SWOT analysis of the hybrid solution.

Table 5-12: SWOT Analysis (hybrid solution).

Strengths	Weaknesses
– Reduces the complexity of the central system configuration (data servers, data centre and applications). – Lower telecommunication infrastructure costs as a result of data decentralisation. – Solution does not introduce a single point of failure due to data and functionality decentralisation. – Visa and traveller verification is conducted in many cases from data stored at national level, thus possible speedier execution.	– Increased complexity of the national system configuration (data servers, data centre and applications). – System development and deployment planning is longer. – System administration and management burden increases, as a result of the number of distributed systems (one fat site per Member State). – System maintenance burden increases as well as the administration of change management procedures. – Business continuity burden increases having to establish and maintain 27 complex systems. – The administration of security becomes more complex (security policies applied to 27 N-VIS locations + C-VIS). – N-VIS should be equipped with complex hardware and software. – Project management, strategic and financial risk increases as a result of the complexities introduced.
Opportunities	**Threats**
– Verification process supported by functions and data stored at national level.	– Much more complex to introduce new Member States with significant impact on strategic risks. – Increasing the complexity at national level (N-VIS) significantly increases technology risks.

5.6 OPTION 2: TECHNICAL INTEGRATION OF VIS AND SIS II

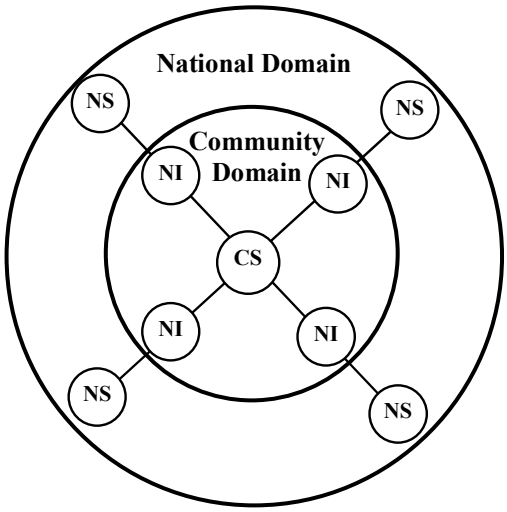
The second option relates to costs savings and operational efficiency as a result of the *technical integration* of the VIS and SIS II systems. Synergies can apply to any architecture of option 1 since synergies do not define a new architecture (neither for the VIS nor for the SIS). In a nutshell, synergies explore what can be shared by the two systems. Possible synergies will be presented below.

Technical integration will be implemented while the two systems are logically kept separate as is required from a legal point of view.

5.6.1 Background

SIS II is the new system expected to replace SIS. Its architecture is depicted in Figure 5-17. SIS II is made of a single core system (CS) to which the various Member States connect their existing national systems (NS) through national interfaces (NI). This architecture is very similar to that of VIS where we can also find a central system (C-VIS), existing national systems (NS) and interfaces between the National Domain and the Community Domain (N-VIS). This similarity naturally demands for an exploration of possible synergies.

Figure 5-17: Architecture of SIS II.



In the business context of visa issuing, police and immigration operations, these two new systems (VIS and SIS II) should solve the following lacks of collaboration:

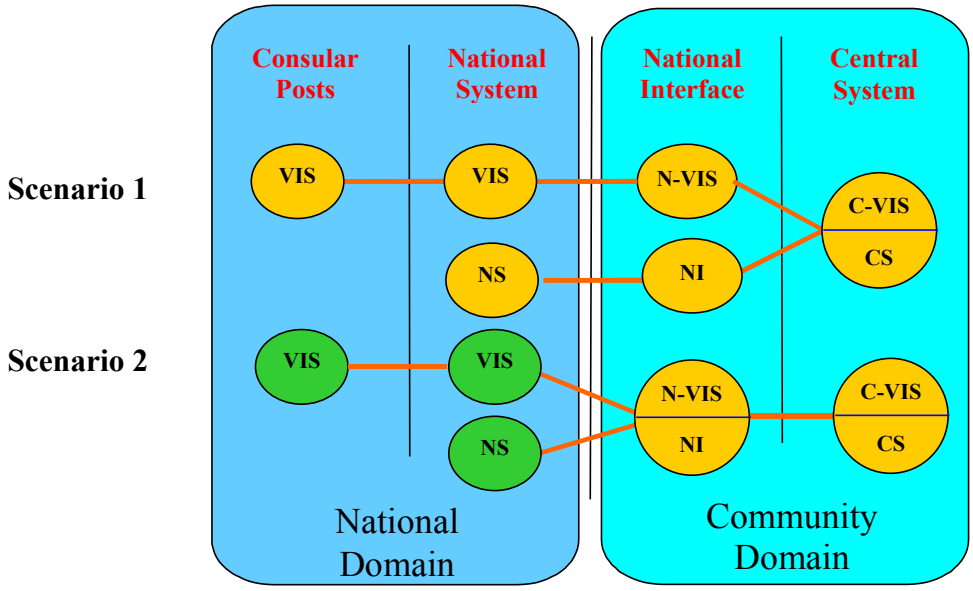
- VIS users (consular posts and other authorities involved in visa issuing) need to check the SIS system in order to verify if an alert has been issued for each visa applicant. This is currently done in consular posts by using CD-ROMs, possibly outdated by more than six weeks. However, some Member States do have on-line connection to the central SIS database. Whilst, for the time being, only the National Central Authorities have access to the SIS database;
- SIS users (border police and immigration departments) need to check visa authenticity, verify traveller identity or identify undocumented travellers. Currently they do not have access to any system that can streamline these processes. However, some Member States do have on-line connections between the border crossing point authorities and the national visa system (only visas issued by that Member State can be checked at border checkpoints). Nevertheless, the VIS database should supply the required information.

5.6.2 Synergies between SIS II and VIS

From a high level viewpoint synergies can be envisaged, and two scenarios are depicted in Figure 5-18:

- **Scenario 1**: sharing the same infrastructure at the *central* level only or
- **Scenario 2**: sharing the same infrastructure at both the *central* and *national interface* levels.

Figure 5-18: VIS and SIS synergy scenarios.



For both scenarios the two systems will remain logically separated (each system will have separately managed access rights).

The first scenario is straightforward as both systems are under the umbrella of a single authority, i.e. the EC. So far no administrative complexity can be seen as being negative. Unfortunately the second scenario should be rejected as national interfaces might not be under the sole responsibility of the EC but would be operated by Member States, possibly by several different national administrations. Therefore, for the time being, **only the first scenario can be considered practical,** and will be examined here.

It is clear that synergies can be established by exploiting similarities between the two systems, however it is necessary to consider possible negative effects, and these considerations create two solutions.

Solution 1: ***common technical platform – independent system lifecycles***

The first solution considers a first level of synergies that keeps the two systems physically separate (no shared hardware or software). This solution allows for *independent system lifecycles* (system development, system set up and system maintenance). Practically, solution 1 envisages the following synergies:

- Locating the two systems in the same building and connecting them to the same private network through a single shared access point;
- Using the same technological platform (and therefore vendors) for both systems:
  - hardware (including biometrics, which leads to using the same biometric identifier for both systems);
  - software;
  - software development framework.
- Maintaining the two systems with a single team;
- Managing the two systems with a single organisation.

Solution 2: ***common technical platform and services – dependent system lifecycles***

The second solution, aimed at increasing the amount of savings, considers **additional** synergies between the two systems. This approach would make the two systems logically and physically inter-related and would not allow for independent life cycles. Practically, the additional synergies envisaged in solution 2 are:

- *System integration*: The hardware and software would be shared between the two systems instead of having each system running on its own dedicated system;
- *Application integration*: Application development would be done with a view to sharing common functions between the two systems.

None of the synergies discussed have an impact on the business processes. Both the SIS and the VIS users will be able to operate seamlessly if the synergies are implemented. Synergies only have an impact on the costs of the systems.

5.6.2.1 Impact of synergies on the information flows

Although the information flow for *visa issuing* remains unchanged[19], the information flows for *visa and traveller verification* and *person identification* (both performed by SIS users) will be optimised as a consequence of the application of solution 1. The new information flows are depicted in Figure 5-19 and Figure 5-20 respectively. They differ from the information flows pertaining to the separate solution for VIS because *the N-VIS and the NI no longer need to be interconnected*[20]. As a consequence, bandwidth savings can be carried out because:

- The networks for interconnecting the NIs to the N-VISes are no longer required anymore;
- The network that will interconnect the C-VIS and the various N-VISes will not carry the traffic for visa and traveller verification, which was the only reason for having a very highly available VIS network (see Chapter 4). Accordingly only cheaper interfaces will be required.

[19] Visa issuing requires that the SIS database be checked, which is always performed seamlessly by the C-VIS on behalf of the VIS users.
[20] SIS users requests will reach the CS directly instead of joining the VIS network at national level.

Figure 5-19: Visa and traveller verification.

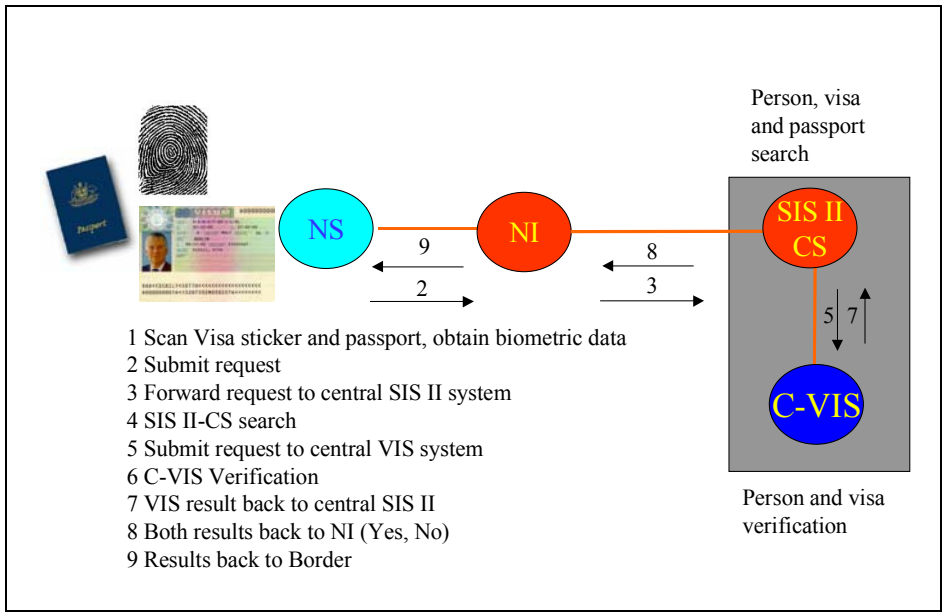
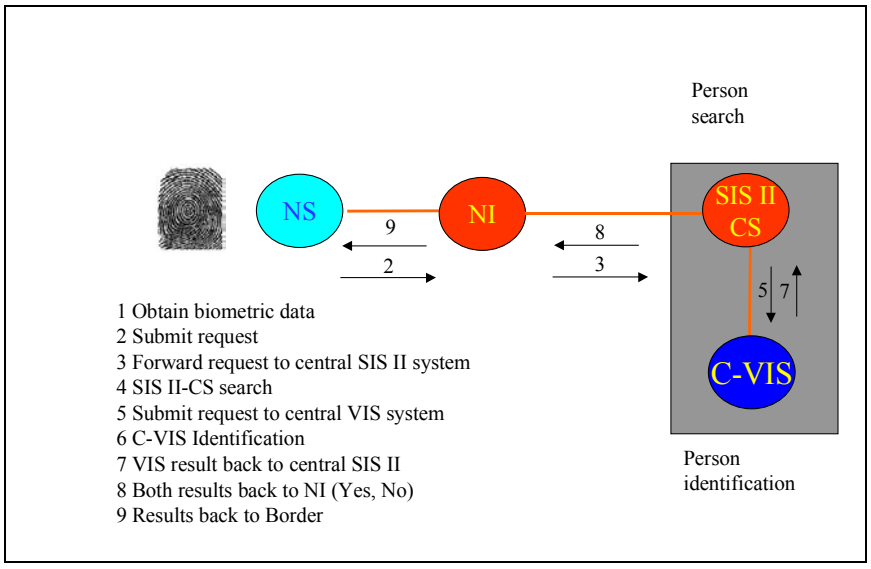
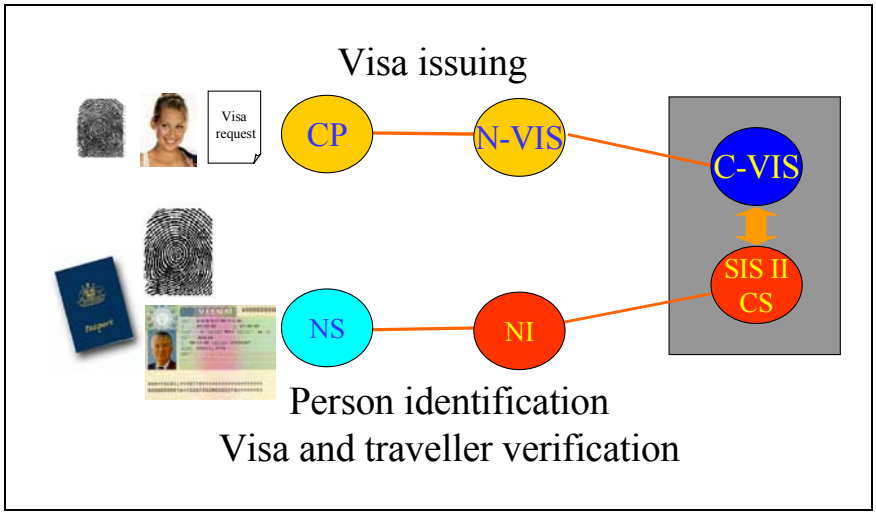


Figure 5-20: Person identification.



As a result of the synergies and information flow modifications, the collaboration between the two systems can be seen as depicted in Figure 5-21.

Figure 5-21: Combined SIS/VIS architecture.



5.6.3 Assessment of the possible solutions

We have reviewed two different levels of synergies that can be applied to option 1/solution 1 with a view to enhancing the organisational and functional performance of the system as well as to saving money. Besides costs savings, which are examined for each solution below, solution 1 (and consequently solution 2) will reduce the overall complexity of managing the two systems since:

- Less network interfaces will be required;
- Less computing rooms will be required;
- Less human resources will be necessary to operate the systems.

Obviously, the main interest in applying the synergies comes from the savings that could be reached. Therefore, we shall further analyse the possible saving centres, the amounts of which will be addressed in Chapter 7 (financial analysis). For the sake of clarity, savings are mentioned for the production systems only but some of them apply to the business continuity systems as well, this will also be reflected in Chapter 7.

Solution 1: ***common technical platform – independent system lifecycles***

In case of the first level of synergy we have the following **costs savings**:

- Renting only one computer room instead of two;
- Avoiding network traffic between the N-VIS and the NI systems. The corresponding bandwidth savings are reported in Table 5-13 for the two envisaged response times and various categories of N-VIS;
- Requiring a lower availability for the network that interconnects the C-VIS and the N-VISes;
- Reducing the amount of human resources required for managing, maintaining and operating the systems;
- Using a single test system instead of two.

Table 5-13: Bandwidth savings (Mbps) between N-VIS and NI resulting from synergies.

Mbps	T1	T2
N-VIS cat. III	0.400	3.2
N-VIS cat. II	0.400	3.2
N-VIS cat. I	0.400	3.2

Solution 2: ***common technical platform and services – dependent system lifecycles***

If the second level of synergy is applied, we have **additional savings** for:

- Hardware and software as some components will be shared;
- Application development as some functions will be common to the two systems.

At this stage no specific drawback is anticipated for solution 1. However, solution 2 introduces dependencies from an operational and technical perspective:

- Common or individual upgrades to either VIS or SIS II will cause considerations on both sides simultaneously and will affect the risks of service disruption.

Accordingly the additional complexity of solution 2 should be balanced with regards to the additional cost savings that would ensue.

6. CANDIDATE COMMUNICATION INFRASTRUCTURE

6.1 INTRODUCTION

The current chapter presents the communication infrastructure requirements for connecting:

1. N-VIS to the C-VIS;

2. Consular posts to the N-VIS.

It examines three alternatives: the use of the existing infrastructures of SISNET, TESTA II or of a new network infrastructure.

The communication requirements have been determined by:

1. The transaction requirements that pertain to the VIS business processes as these have been determined in chapter 2;

2. The availability requirements as these have been determined in section 4.3.1.1;

3. The contingency planning requirements of section 4.3.1.2;

4. The response time scenarios as documented in section 4.3.1.3.

The communication capacities are documented separately for alphanumeric data, photograph, biometric and supporting documents.

Before introducing the bandwidth requirements, the existing communication infrastructures and in particular those of SISNET and TESTA II are examined.

6.2 COMMUNICATION INFRASTRUCTURES

6.2.1 SISNET

SISNET is a virtual private network that interconnects VISION and SIS users only, and which is managed by the Council, whereas the Central SIS authorities administer the encryption. It is a basic network, with the backbone supplied by Equant, whilst a single provider covers local operations for the access points.

The network relies on the standards-based Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. Its primary service characteristics are:

- Trans-European coverage;
- Meshed network providing any-to-any connectivity;
- Backbone access allowed via dial-up, leased lines connectivity;
- Provides strong encryption and contractual availability of 99.7 % (4 weeks slide window) if Mission Critical access points are used.

The network availability and problem in opening its services to new applications are the major drawbacks in the VIS context.

1. With regards to network availability, SISNET's availability has been measured between 99.5% to 99.7%;

2. With regards to opening its services, SISNET is a closed application network, used only for the SIS II and VISION networks.

6.2.2 TESTA II

TESTA II is a virtual private network that interconnects national, regional or local administrative networks to enable trans-European data interchange. TESTA is currently managed by DG-Enterprise under the IDA program.

It is a state-of-the-art network, with a backbone provided by Equant and local operators for the access points. The network relies on the standards-based Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. The network is not connected to the Internet. Primary service characteristics are:

- trans-European coverage;
- designed for connecting single users, single administrations, and networks of administrations in a closed user group (CUG);
- any-to-any connectivity;
- support of different classes of services managed by different Service Level Agreements (SLA);
- backbone access allowed via dial-up, leased lines and satellite connectivity;
- built-in security features (access control, physical separation from the Internet); additional cryptographic services are available, and firewall services on-demand;
- value-added services including Electronic mail (e-mail), Domain Name Server (DNS), web repository and web hosting services, PKI.

From a security, availability and bandwidth perspectives, TESTA is similar to SISNET. For the backbone, TESTA is equivalent to the SISNET network from a technical point of view. In other areas the architectures differ, as is the case for the local domain.

The network availability, its openness to new application, the added-value services and the possibility to have the service level agreement tailor-made to the project are critical factors to be considered in the context of the VIS:

1. Unlike SISNET, TESTA supports added value services like a public key infrastructure, e-mail relay or web hosting which could be used by the VIS;

2. TESTA is also open to any new application that would like to connect, making each national access point shared by a potentially unlimited number of applications. EURODAC and Dublin-Net are currently using TESTA II. Nevertheless, it is a far less binding environment compared to the SISNET, which is a closed application environment dedicated to SIS and VISION applications;

3. TESTA services can become available to any new application, such as the VIS, under a service level agreement specific to the project;

4. The availability of TESTA ranges from 99.5% to 99.7% monthly as indicated in Table 6-1.

Table 6-1: Availability of TESTA II.

Service element	Minimum Availability
EuroGate services at all locations.	99.7% monthly, 99.9% yearly
On-net access to an EuroGate.	99.7% monthly, 99.9% yearly
Off-net access to an EuroGate.	99.7% monthly with back-up
Web site platform.	99.5% monthly
Firewall service.	99.5% monthly
Cryptography services.	99.7% monthly

6.2.3 New network infrastructure

From a technical perspective the use of a new network is a feasible option, however there are no obvious advantages attached to this. Procuring a new networking infrastructure will increase the financial and human resources burden and will introduce project management risks as sourcing and roll-out of this new network requires considerable time (SISNET has required 18 months to be set up). The procurement of a new infrastructure should be carefully assessed with regards to the evolution of TESTA. DG-Enterprise has initiated the upgrade of the network (TESTA III) through a public procurement procedure contractually to begin on the 1st of January 2005. TESTA III could be considered as the new communication infrastructure.

6.3 COMMUNICATION INFRASTRUCTURE – GLOBAL PERSPECTIVE

With regards to the solutions for the VIS architecture, described in Chapter 5, the VIS communication infrastructure requires interconnecting three types of sites:

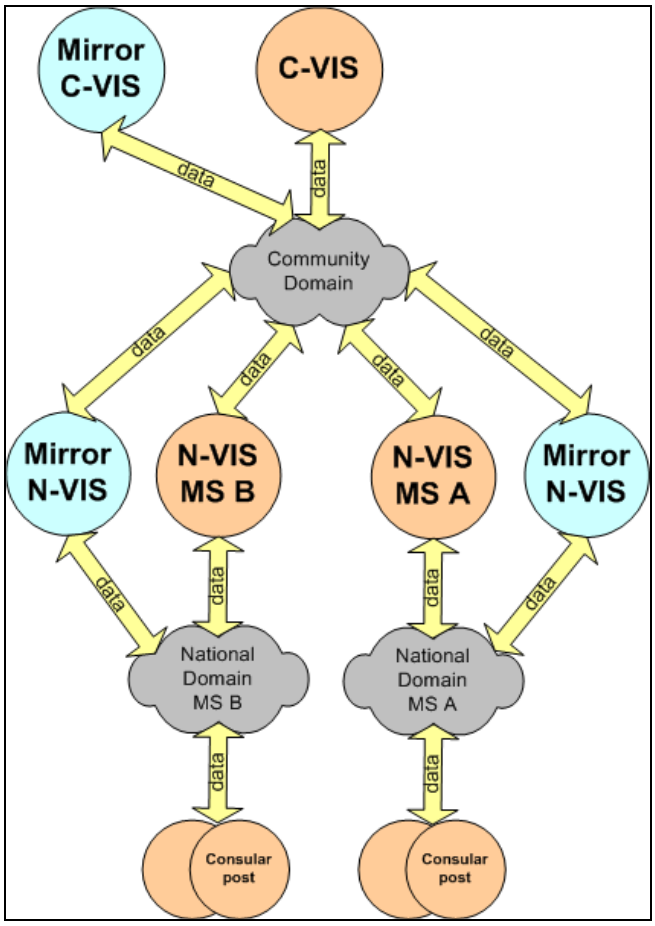
- The Central Visa Information System, **C-VIS site**, which will be located inside the Schengen area. C-VIS is backed-up by a distant identical system for business continuity purposes. The site that hosts the business continuity system is referred to as the mirror site, while a site that hosts the main system is named a production site;
- The various **N-VIS sites**, one located in each Member State. Each N-VIS is backed-up by a distant identical system for business continuity purposes;
- The **consular posts,** which are located world-wide, connected to the N-VIS.

The VIS architecture requires interconnecting the C-VIS and the N-VISes in a single networking infrastructure. This communication infrastructure **will be referred to as the Community Domain, and falls under the responsibility of the EC services.**

Consular posts and other national authorities should connect to the N-VIS to access the VIS services. The network that will provide this connectivity is referred to as the **National Domain**. **This domain falls under the responsibility of each Member State.**

Figure 6-1 illustrates, from a global perspective, the communication infrastructure between the end-user (consular posts and other national authorities) and the N-VIS as well as the C-VIS. Note that the mirror sites pose the same communication infrastructure connectivity requirements as the production sites. Connectivity between an N-VIS and its mirror site will occur through their connections to the Community Domain.

Figure 6-1: VIS networking architecture.



Legend:
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)

The connectivity between C-VIS and N-VIS as well as between Consular posts and N-VIS is further analysed below.

6.4 COMMUNICATION INFRASTRUCTURE BETWEEN N-VIS AND C-VIS

VIS is a mission-critical application that stores and manages sensitive information (visa data, biometrics, photographs). In this respect, the following are applicable for the Community Domain:

- The communication between the C-VIS and N-VISes should be established over a virtual private network using strong **encryption**;
- The **availability** of this communication network should meet to the requirements drawn in chapter 4, Table 4-2;

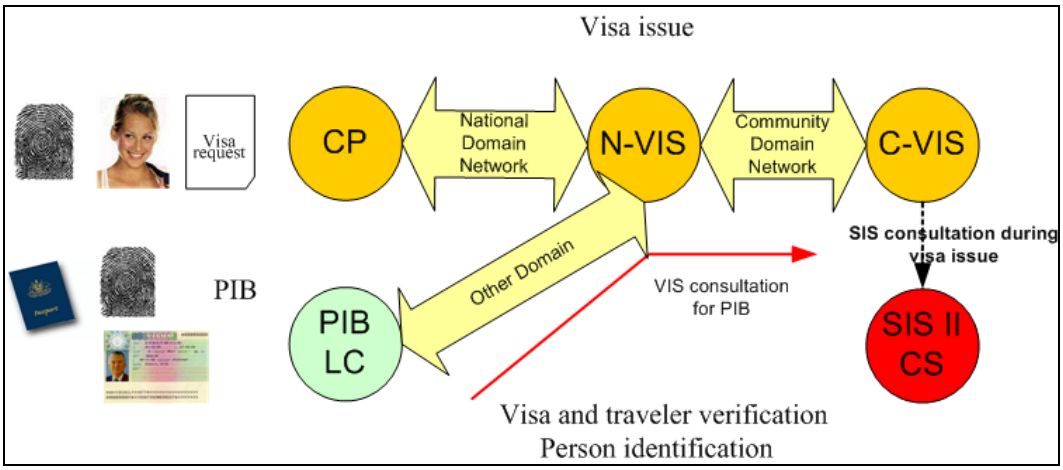
- Each Member State should facilitate two access points[21] (one at the N-VIS site and the other at the mirror N-VIS site) with sufficient **bandwidth capacity to support the VIS business context (processes and transactions) determined in chapter 2**.

Keeping Figure 6-1 in mind, below the suitability of SISNET or TESTA for the options and solutions of the VIS is examined below.

6.4.1 Option 1: Centralised solution

Figure 6-2 illustrates the high-level communication infrastructure architecture concerning the centralised solution. Police, immigration and border checkpoint authorities use the VIS communication infrastructure for visa and traveller verification and person identification.

Figure 6-2: Communication architecture for the centralised solution.



Legend:
CP refers to **C**onsular **P**ost
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities, which could possibly be the **NI** of the SIS II
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
SIS II CS refers to the **c**ore **s**ystem of the SIS II.

From a technical perspective this solution requires large bandwidth at the C-VIS due to the centralised storage of the data (alphanumeric, photograph, biometrics, supporting documents).

To support the VIS business processes, determined in table 4-1, a 99.9% availability is required to support the critical process of *visa and traveller verification*. Similarly for the less critical processes of *visa issue* and *person identification*, an availability of 99.7% is required.

Currently SISNET and TESTA have 99.7% availability. Therefore, these networks do not contractually support the required availability of the *visa and traveller verification* at a border checkpoint. However, they can fully support the less critical processes of *visa issue* and *person identification*. Table 6-2 benchmarks SISNET and TESTA against the business process availability requirements for the VIS processes.

[21] An access point is a device that interconnect a local area network (an N-VIS for instance) to a wide area network (the Community Domain for instance).

Table 6-2: Benchmarking of the communication infrastructure between N-VIS and C-VIS.

Business Process	TESTA II	SISNET
Visa issue	Suitable	Suitable
Visa and traveller verification	Not Suitable	Not Suitable
Person identification	Suitable	Suitable

SISNET or TESTA would have to be upgraded to meet the bandwidth requirements of the centralised solution. The use of the VIS infrastructure to support the *visa and traveller verification* performed by the PIB authorities imposes a strict 99.9% availability requirement for the network connecting C-VIS to N-VIS.

Neither SISNET nor TESTA II meet the required business process availability of 99.9% for the visa and traveller verification process. **Therefore the use of a new communication infrastructure should be considered.**

6.4.2 Option 1: Hybrid solution

The communication infrastructure architecture is identical to the one illustrated in Figure 6-3. However, in the hybrid solution the bandwidth requirements at the C-VIS are much lower due to data decentralisation. It is therefore technically feasible to upgrade SISNET or TESTA to meet the bandwidth requirements for the hybrid solution.

From an availability perspective, neither SISNET nor TESTA can support the visa and traveller verification process. However, they can fully support the less critical processes of *visa issue* and person identification. Table 6-3 benchmarks SISNET and TESTA against the business process availability requirements for the VIS processes.

Table 6-3: Benchmarking of the communication infrastructure between N-VIS and C-VIS.

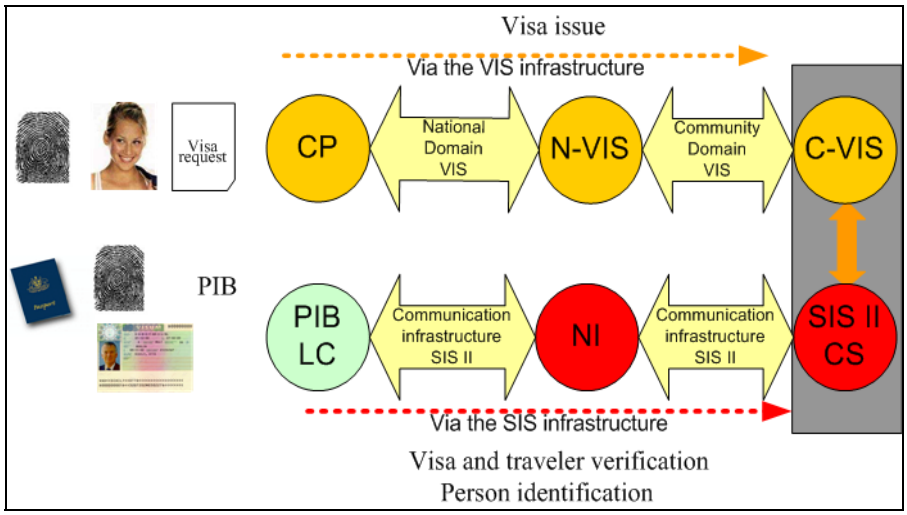
Business Process	TESTA II	SISNET
Visa issue	Suitable	Suitable
Visa and traveller verification	Not Suitable	Not Suitable
Person identification	Suitable	Suitable

Concerning the required availability, neither SISNET nor TESTA II meet the required business process availability of 99.9% for the *visa and traveller verification process*. **Therefore the use of a new communication infrastructure should be considered.**

6.4.3 Option 2: Synergies between VIS and SIS II

Figure 6-3 illustrates the communication infrastructure architecture where synergies are introduced between the VIS and SIS II at central level. Police, immigration and border checkpoint authorities use the communication infrastructure of the future SIS II for visa and traveller verification and person identification. Similarly, consular posts connect to the VIS infrastructure for the visa issue procedures.

Figure 6-3: Communication architecture (synergies between VIS and SIS II).



Legend:
CP refers to **C**onsular **P**ost
N-VIS refers to the **n**ational **v**isa **i**nformation **s**ystem (the national component of the VIS)
C-VIS refers to the **c**entral **v**isa **i**nformation **s**ystem (the central component of the VIS)
PIB LC refers to a **l**ocal **c**onfiguration operated by the **PIB** authorities
PIB refers to **p**olice, **i**mmigration and **b**order checkpoint authorities
NI refers to the **n**ational **i**nterface of the SIS II
SIS II CS refers to the **c**ore **s**ystem of the SIS II.

As a result of the synergies between the VIS and SIS II:

1. The network availability of the VIS communication infrastructure (N-VIS to C-VIS) is relaxed to 99.7% **as it is only used to run the less critical process of *visa issue***;

2. The SIS II communication infrastructure should provide an availability of 99.9%. The *verification* and *identification* business processes run on the SIS II communication infrastructure, thus lowering the bandwidth requirements of the VIS communication infrastructure.

In view of the above, Table 6-4 benchmarks SISNET and TESTA against the business process availability requirements for the VIS processes.

Table 6-4: Benchmarking of the communication infrastructure between N-VIS and C-VIS.

VIS Business Process	TESTA II	SISNET
Visa issue	Suitable	Suitable
Visa and traveller verification	SIS infrastructure	SIS infrastructure
Person identification	SIS infrastructure	SIS infrastructure

SISNET and TESTA are suitable for providing the N-VIS to C-VIS connectivity to support the visa issuance process, which requires an availability of 99.7%. However, networks will have to be upgraded in terms of bandwidth capacity.

The SIS II communication infrastructure should be upgraded to provide 99.9% availability required by the critical process of visa and traveller verification and person identification.

6.4.4 Conclusions communication infrastructure (N-VIS to C-VIS).

Concerning **option 1**, the separate VIS:

1. The existing networks, SISNET or 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;

2. Upgrading the existing network infrastructures, SISNET or TESTA to meet the requirements of the *centralised* or hybrid *solution* is a feasible option from a technical perspective. It has however to be based upon a new Service Level Agreement (SLA) with a service provider that will ensure monthly network availability of 99.9%. In the SISNET case it is difficult to draw up a new contract (and thus SLA) given that the current contractual arrangements expire in 2008 and cannot be extended. **Moreover, it will be difficult to create a legal basis and open SISNET to the VIS application, thus SISNET should not be seen as a candidate communication infrastructure for the VIS.** Similarly, in the case of TESTA II its contract expires in 2005, before the VIS system is put into production. However, TESTA III would be available in 2005 in parallel with the development of the VIS;

3. **Therefore, in the separate solution it is recommended to opt for a complete new communication infrastructure. The total set-up time for this new infrastructure will be at least 18 months**. **The best option is to use the future TESTA III as the new network as DG-Enterprise has initiated the upgrade of the TESTA II network through a public procurement procedure to be launched 4th Quarter 2003. The TESTA III procurement contract should be prepared to meet the required availability requirements of the VIS and the SIS II.**

Concerning **option 2:** the technical integration between the VIS and SIS II:

1. The synergies at end-user level require the upgrade of the SIS communication infrastructure to accommodate the extra traffic for *visa and traveller verification* and *person identification* and thus to provide a network availability of 99.9%;

2. The VIS communication infrastructure, connecting C-VIS and N-VIS, could be streamlined either via SISNET or TESTA II as each network provides an availability of 99.7%. **However, it will be difficult to create a legal basis and open SISNET to the VIS application, thus SISNET should not be seen as a candidate communication infrastructure for the VIS. Therefore, the openness of TESTA (with regards to new applications) prevails;**

3. Synergies drive for a common infrastructure to be used by VIS and the SIS II. Thus a new network will have to be established in order to meet the communication requirements drawn in chapter 4, including the required availability of 99.9%. **An option would be to use the future TESTA III as the common network both for SIS and the VIS.**

6.5 COMMUNICATION INFRASTRUCTURE BETWEEN N-VIS AND CONSULAR POSTS

The sensitivity of the VIS information and the critical aspect of the VIS services require the following for the National Domains:

1. They should be closed networks using strong encryption. The reported figure does not include the bandwidth overheads as a result of the encryption process. Member States can implement cryptographic techniques of their choice, and thus have to derive (scale-up) the required bandwidth accordingly;

2. Recommended availability compliant with Table 4-2.

Each consulate should be connected to its **National Domain** with a sufficient **bandwidth** and each Member State should have two access points (one at the N-VIS site and the other at the mirror N-VIS site) connected to its **National Domain** with a sufficient bandwidth. This bandwidth is reported in Table 6-5 (for consulates) and in Table 6-6 [22] for the three categories of N-VIS.

Figures are cumulative, starting with the alphanumeric data, then adding photographs, biometric identifiers and finally supporting documents have been assumed. Figures for the two response times have been considered and documented separately.

Table 6-5: Required bandwidths (kbps) for the National Domains access points in consulates.

Location	Alphanumeric data	+photographs	+biometrics	+documents
Response time T_1 (normal)				
Consulate cat. III	1 (~0%)	12 (100%)	12 (100%)	19 (100%)
Consulate cat. II	1 (~0%)	5 (20%)	5 (20%)	5 (40%)
Consulate cat. I	1 (~0%)	5 (0%)	5 (~0%)	5 (~0%)
Response time T_2 (fast)				
Consulate cat. III	1 (~0%)	40 (30%)	40 (30%)	40 (50%)
Consulate cat. II	1 (~0%)	40 (2%)	40 (2%)	40 (5%)
Consulate cat. I	1 (~0%)	40 (~0%)	40 (~0%)	40 (~0%)

Legend: Figure in brackets denotes the average usage of the bandwidth capacity. **The under-utilisation of the bandwidth is the result of having to meet the response time requirements poses by the business processes (refer to Table 4-2).**

The required bandwidth depends on the response time. This is because the requirement is to send information as fast as possible in order to comply with the response time of the business processes. Therefore, there is no difference shown between small and large consulates. As a consequence, the telecommunication lines remain inactive.

As an example, let us consider a consulate of Category I and response time scenario T1 (normal). An initial capacity of 1kbps is needed to transmit alphanumeric data to the N-VIS. However, due to the very small number of visas handled by this type of consular post (500 visas per year), the bandwidth utilisation rate is near to zero (~0%). To support the transmission of photographs to the N-VIS, the commutative capacity has to be of 5 kbps, whereas the line utilisation still remains at near to zero levels (~0%). The same more or less applies for biometrics and supporting documents. Thus the communication capacity increases to meet the business process response time. However, due to the small number of visas to be issued, the bandwidth utilisation rate is small, near to zero (~0%).

Consider now a consulate of Category III and response time scenario T1 (normal). An initial capacity of 1kbps is needed to transmit alphanumeric data to the N-VIS. However, as alphanumeric data is low in volumes, the bandwidth utilisation rate is near to zero (~0%). To

[22] The bandwidths assume a worst case scenario regarding the number of fingerprints (10) and biometric accuracy. Significant savings could occur if the biometric accuracy proves to be sufficient, eliminating the need to use photographs for identification.

support the transmission of photographs to the N-VIS, the cumulative capacity has to be 12 of kbps. A line utilisation rate of 100% shows that the large amount of visas handled by consulates of Category III determines the line capacity and de facto satisfies the response time T1. The same more or less applies for biometrics and supporting documents. Thus the communication capacity increases (as we introduce new data components) to meet the volume requirements**.**

Table 6-6: Required bandwidths (Mbps) for the National Domains access points in N-VISes.

Location	Alphanumeric data	+photographs	+biometrics	+documents
Response time T_1 (normal)				
N-VIS cat. III (or mirror)	0.064	1.536	1.536	1.664
N-VIS cat. II (or mirror)	0.064	0.384	0.448	0.448
N-VIS cat. I (or mirror)	0.064	0.384	0.448	0.448
Response time T_2 (fast)				
N-VIS cat. III (or mirror)	0.064	3.000	3.200	3.200
N-VIS cat. II (or mirror)	0.064	3.000	3.200	3.200
N-VIS cat. I (or mirror)	0.064	3.000	3.200	3.200

The bandwidth capacity connecting N-VIS to the national domain is driven by the response time requirements of the business processes. The communication capacity to connect N-VIS to the national domain is independent of the solution for the architecture (centralised or hybrid). Regardless of the selected architecture, the same amount of data (throughput) will have to be transmitted from the consular posts to the N-VIS.

6.5.1 Conclusions on the Communication infrastructure between N-VIS and consular posts

Member States according to the number of the local systems per category I, II and III (refer to section 4.3.4) can procure the required bandwidth to support the VIS business context. Table 6-5 facilitates the communication infrastructure procurement procedure. The required bandwidths for connecting consular posts to the N-VIS remain level and should be available in most countries, through terrestrial or satellite networks.

Member States with communication infrastructures in place, connecting their consular posts to national visa systems, have to assess if the existing capacity and availability are sufficient (chapter 4 Table 4.1) according to the above requirements (Table 6-5 to be used for this assessment).

Similarly, Member States can determine their communication infrastructure costs for connecting their N-VIS to the national domain using the figures provided in Table 6-6. It is the responsibility of each Member State to set up and maintain its National Domain and the access points to it. This should not be a major issue for access points located in the Schengen countries (see SISNET and TESTA examples).