Commission Decision of 17 June 2008 laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase (notified under document number C(2008) 2693) (Only the Bulgarian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish texts are authentic) (2008/602/EC)

COMMISSION DECISION

of 17 June 2008

laying down the physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase

(notified under document number C(2008) 2693)

(Only the Bulgarian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish texts are authentic)

(2008/602/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS)[1], and in particular Article 4(a) thereof,

Whereas:

(1) Decision 2004/512/EC established the VIS as a system for the exchange of visa data between Member States and gave the mandate to the Commission to develop the VIS.

(2) Appropriate arrangements, in particular as regards the elements of the national interface located in each Member State, should be put in place between the Commission and the Member States.

(3) In accordance with Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*[2], the United Kingdom has not taken part in the adoption of Decision 2004/512/EC and is not bound by it or subject to its application as it constitutes a development of provisions of the Schengen *acquis*. The United Kingdom is therefore not an addressee of this Commission Decision.

(4) In accordance with Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis*[3], Ireland has not taken part in the adoption of Decision 2004/512/EC and is not bound by it or

subject to its application as it constitutes a development of provisions of the Schengen *acquis*. Ireland is therefore not an addressee of this Commission Decision.

(5) Pursuant to Article 5 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and the Treaty establishing the European Community, on 13 August 2004 Denmark decided to implement Decision 2004/512/EC in Danish law. Decision 2004/512/EC is thus binding upon Denmark in international law. Denmark has therefore an obligation under international law to implement this Decision.

(6) As regards Iceland and Norway, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters association with the implementation, application and development of the Schengen *acquis*[4], which fall within the area referred to in Article 1, point B of Council Decision 1999/437/EC of 17 May 1999[5] on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis*.

(7) As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement signed by the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1, point B of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[6] on the conclusion of that Agreement on behalf of the European Community.

(8) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1, point B of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/261/EC of 28 February 2008 on the signature, on behalf of the European Community, and on the provisional application of certain provisions of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[7].

(9) The measures provided for in this Decision are in accordance with the opinion of the Committee set up by Article 5(1) of Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II)[8],

HAS ADOPTED THIS DECISION:

Article 1

The physical architecture and requirements of the national interfaces and of the communication infrastructure between the central VIS and the national interfaces for the development phase shall be as set out in the Annex.

Article 2

This Decision is addressed to the Kingdom of Belgium, the Republic of Bulgaria, the Czech Republic, the Federal Republic of Germany, the Republic of Estonia, the Hellenic Republic, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Grand Duchy of Luxembourg, the Republic of Hungary, the Republic of Malta, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Slovenia, the Slovak Republic, the Republic of Finland and the Kingdom of Sweden.

Done at Brussels, 17 June 2008.

For the Commission

Jacques BARROT

Vice-President

ANNEX

1. Introduction

This document describes the network requirements and the design of the communication infrastructure and its components.

1.1. Acronyms and abbreviations

Acronyms and abbreviations	Explanation
BCU	Backup central unit
BLNI	Backup local national interface
CNI	Central national interface
CS	Central system
CS-VIS	Central visa information system
CU	Central unit
DNS	Domain name server
FTP	File transfer protocol
HTTP	Hypertext transfer protocol
IP	Internet protocol
LAN	Local area network
LNI	Local national interface
NI-VIS	National interface
NTP	Network time protocol
SAN	Storage area network
SDH	Synchronous digital hierarchy
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
sTESTA	Secure Trans-European Services for Telematics between Administrations, is a measure of the IDABC programme (interoperable delivery of pan-European eGovernment services to public administrations, business and citizens. Decision of the European Parliament and Council 2004/387/EC[a]).
TCP	Transmission control protocol
VIS	Visa information system
VPN	Virtual private network

a OJ L 181, 18.5.2004, p. 25.

WAN	Wide area network

a OJ L 181, 18.5.2004, p. 25.

2. Physical architecture of the national interfaces and of the communication infrastructure between the central VIS and national interfaces

The NI-VIS, as defined in Article 1(2) of Council Decision 2004/512/EC, shall consist of:

— one local national interface (hereinafter referred to as 'LNI') for each Member State which is the interface that physically connects the Member State to the secure communication network and contains the encryption devices dedicated to VIS. The LNI is located at the Member State premises,

— an optional backup local national interface (hereinafter referred to as 'BLNI') which has the same content, function as the LNI.

The specific configuration of the LNI and BLNI will be specified and agreed with each individual Member State.

The LNI and BLNI are to be used exclusively for purposes defined by the Community legislation applicable to VIS.

The communication infrastructure between the CS-VIS and the NI-VIS shall consist of:

— the network for Secure Trans-European Services for Telematics between Administrations (sTESTA) that provides an encrypted, virtual, private network (vis.stesta.eu) dedicated to VIS data and to communication between Member States according to the Community legislation related to VIS and between Member States and the authority responsible for the operational management for the CS-VIS.

3. Network services

In chapters 3, 5 and 7, whenever technologies or protocols are mentioned, it should be understood that equivalent technologies or protocols may be used. The deployment of the network shall take into account the readiness of Member States.

3.1. Network layout

The VIS architecture makes use of centralised services, which are accessible from the different Member States. For resiliency purposes these centralised services are duplicated to two different locations namely Strasbourg, France, hosting the principal CS-VIS, central unit (CU) and St Johann im Pongau, Austria, hosting the backup CS-VIS, backup central unit (BCU) in accordance with Commission Decision 2006/752/EC of 3 November 2006 establishing the sites for the Visa Information System during the development phase[9].

The principal and backup central units shall be accessible from the different Member States via network access points – an LNI and a BLNI – interconnecting their national system to the CS-VIS.

The connection between the principal CS-VIS and the backup CS-VIS shall be open for any new future architectures and technologies and shall allow for the continuous synchronisation between the CU and BCU.

3.2. Bandwidth

The bandwidth needed for the LNI and the optional BLNI may be different from one Member State to another.

The communication infrastructure shall offer site connection bandwidths adapted to the expected traffic load. The network shall supply sufficient minimal guaranteed upload and download speeds for each connection and it shall support the total bandwidth size of the network access points.

3.3. Supported protocols

The communication infrastructure shall be able to support network protocols used by the CS-VIS, in particular HTTP, FTP, NTP, SMTP, SNMP, DNS, tunnelling protocols, SAN replication protocols and the proprietary Java-to-Java connection protocols of BEA WebLogic over IP.

3.4. Technical specifications

3.4.1. IP addressing

The communications infrastructure shall have a range of reserved IP addresses that may solely be used within that network. Within the reserved IP range, the CS-VIS will use a dedicated set of IP addresses that will not be used elsewhere.

3.4.2. Support for IPv6

The local networks of most sites will be using IPv4 but some may use IPv6. Therefore the network access points shall offer the possibility to act as a IPv4/IPv6 gateway. Coordination with Member States evolving towards IPv6 will be required, in order to ensure a smooth transition.

3.4.3. Sustained flow rate

As long as the CU or BCU connection has a load rate less of 90 %, a given Member State shall be able to sustain continually 100 % of its specified bandwidth.

3.4.4. Other specifications

To support the CS-VIS, the communication infrastructure shall at least comply with a minimum set of technical specifications:

The transit delay shall be (including the busy hours) less or equal to 150 ms in 95 % of packets and less than 200 ms in 100 % of packets.

Its probability of packet loss shall be (including the busy hours) less or equal to 10^{-4} in 95 % of packets and less than 10^{-3} in 100 % of packets.

The aforementioned specifications apply to each access point separately.

The connection between the CU and BCU shall have a round trip delay less or equal to 60 ms.

3.5. Resiliency

The communication infrastructure shall offer high availability, in particular of the following components:

— backbone network,
— routing devices,
— points of presence,
— local loop connections (including physically redundant cabling),
— security devices (crypto devices, firewalls, etc.),
— all generic services (DNS, etc.),
— LNI and optional BLNI.

Network failover mechanisms shall be set up and, when required, coordinated with the application level to ensure maximum availability of the VIS as a whole.

4. Monitoring

To facilitate monitoring, the communication infrastructure's monitoring tools shall have the capability to be integrated with the monitoring facilities for the operational management of the CS-VIS.

5. Generic services

The communication infrastructure shall be able to offer the following optional generic services: DNS, mail relay and NTP.

6. Availability

The availability of connection points up to the LAN of the communication infrastructure shall be 99,99 % over a 28-day rolling period.

7. Security services

7.1. Network encryption

No VIS-related information shall circulate on the communication infrastructure without encryption.

To maintain a high level of security, the communication infrastructure shall allow managing the certificates/keys used by the network encryption solution. Remote administration and remote monitoring of the encryption boxes shall be possible.

Symmetric encryption algorithms (3DES 128 bits or better) and asymmetric encryption algorithms (RSA 1 024 bit modulus or better) shall be used in accordance with the state of the art.

7.2. Other security features

Besides protecting the VIS network access points (LNI and BLNI), the communication infrastructure shall also protect the optional generic services. In case such services are made available, they should meet protection measures comparable to those in CS-VIS. Furthermore, the generic services devices and its protection measures should be under continuous security surveillance.

In order to maintain a high level of security, the communication infrastructure shall allow all security incidents to be reported without any delay. Reports on all security incidents shall be provided on a regular basis, e.g. monthly reporting and ad-hoc basis.

8. Helpdesk and support structure

A helpdesk and support structure shall be established and shall be able to interact with the CS-VIS.

9. Interaction with other systems

The communication infrastructure shall ensure that data leakage towards other systems or other networks will not occur on the network.

(**1**) OJ L 213, 15.6.2004, p. 5.

(**2**) OJ L 131, 1.6.2000, p. 43.

(**3**) OJ L 64, 7.3.2002, p. 20.

(**4**) OJ L 176, 10.7.1999, p. 36.

(**5**) OJ L 176, 10.7.1999, p. 31.

(**6**) OJ L 53, 27.2.2008, p. 1.

(**7**) OJ L 83, 26.3.2008, p. 3.

(**8**) OJ L 328, 13.12.2001, p. 4. Regulation as amended by Regulation (EC) No 1988/2006 (OJ L 411, 30.12.2006, p. 1).

(**9**) OJ L 305, 4.11.2006, p. 13.