COMMISSION DECISION

of 16 March 2007

laying down the network requirements for the Schengen Information System II (3rd pillar)

(2007/171/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty on European Union,

Having regard to Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation of the Schengen Information System (SIS II) [1], and in particular Article 4(a) thereof,

Whereas:

(1) In order to develop SIS II it is necessary to set out technical specifications concerning the communication network, its components, and the specific network requirements.

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

(3) This Decision is without prejudice to the adoption in future of other Commission Decisions related to the development of SIS II, in particular on the development of the security requirements.

(4) Both Council Regulation (EC) No 2424/2001 [2] and Decision 2001/886/JHA govern the development of the SIS II. In order to ensure that there will be one single implementing process for the development of SIS II as a whole, the provisions of this Decision should mirror the provisions of the Commission's Decision laying down the network requirements for SIS II to be taken in application of Regulation (EC) No 2424/2001.

(5) The United Kingdom is taking part in this Decision, in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 8(2) of 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* [3].

(6) Ireland is taking part in this Decision in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 5(1) and 6(2) of 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* [4].

(7) As regards Iceland and Norway, this Decision constitutes a development of the 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 association of those two States with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC [5] on certain arrangements for the application of that Agreement.

(8) As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement signed between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis*, which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC read in conjunction with Article 4(1) of Council Decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement [6].

(9) This Decision constitutes an act building on the Schengen *acquis* or otherwise related to it within the meaning of Article 3(1) of the Act of Accession.

(10) The measures provided for in this Decision are in accordance with the opinion of the Committee set up by Article 5(1) of Decision 2001/886/JHA,

[1] OJ L 328, 13.12.2001, p. 1.

[2] 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).

[3] OJ L 131, 1.6.2000, p. 43. Decision as amended by Decision 2004/926/EC (OJ L 395, 31.12.2004, p. 70).

[4] OJ L 64, 7.3.2002, p. 20.

[5] OJ L 176, 10.7.1999, p. 31.

[6] OJ L 368, 15.12.2004, p. 26.

HAS DECIDED AS FOLLOWS:

Article 1

The technical specifications related to the design of the physical architecture of the communication infrastructure of the SIS II shall be as set out in the Annex.

Done at Brussels, 16 March 2007.

For the Commission
Franco FRATTINI
Vice-president

ANNEX

CONTENTS

1. Introduction

This document describes the design of the communication network, its included components and the specific network requirements.

1.1. *Acronyms and abbreviations*

This section describes the acronyms used throughout the document.

Acronyms and abbreviations	Explanation
BLNI	Backup Local National Interface
CEP	Central End Point
CNI	Central National Interface
CS	Central System
CS-SIS	Technical support function containing the SIS II database
DNS	Domain Name Server
FCIP	Fibre Channel over IP
FTP	File Transport Protocol
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
LNI	Local National Interface
Mbps	Megabits per second
MDC	Main Developer Contractor
N.SIS II	The national section in each Member State
NI-SIS	A uniform national interface
NTP	Network Time Protocol
SAN	Storage Area Network
SDH	Synchronous Digital Hierarchy
SIS II	Schengen Information System, second generation
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
s-TESTA	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 of 21.4.2004).
TCP	Transmission Control Protocol
VIS	Visa Information System
VPN	Virtual Private Network
WAN	Wide Area Network

2. General overview

The SIS II is composed of:

— the central system (hereinafter referred to as 'the Central SIS II') consists of:

- a technical support function (herein after referred to as 'CS-SIS') containing the SIS II database. The principal CS-SIS carries out technical supervision and administration and a backup CS-SIS is capable of ensuring all functionalities of the principal CS-SIS in case of failure of this system,
- a uniform national interface (hereinafter referred to as 'NI-SIS');

— a national section (hereinafter referred to as 'N.SIS II') in each of the Member States, consisting of the national data systems which communicate with the Central SIS II. An N.SIS II may contain a data file (hereinafter referred to as 'national copy'), containing a complete or partial copy of the SIS II database,

— a communication infrastructure between the CS-SIS and the NI-SIS (hereinafter referred to as 'Communication Infrastructure') that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between Sirene Bureaux.

The NI-SIS which consists of:

— one Local National Interface (hereinafter referred to as 'LNI') in each Member State which is the interface that physically connect the Member State to the secure communication network and contain the encryption devices dedicated to SIS II and Sirene traffic. The LNI is located at the Member State premises,

— an optional Backup Local National Interface (hereinafter referred to as 'BLNI') which has exact the same content and function as the LNI.

The LNI and BLNI are to be used exclusively by the SIS II system and for Sirene exchange. The specific configuration of the LNI and BLNI will be specified and agreed with each individual Member State in order to take account of security requirements, the physical location and conditions of installation, including the provision of services by the network provider, meaning the physical s-TESTA connection may contain several VPN tunnels for other systems, for example VIS and Eurodac.

— a Central National Interface (hereinafter referred to as 'CNI') which is an application securing access to the CS-SIS. Each Member State has separate logical access points to the CNI via a central firewall.

The Communication Infrastructure between the CS-SIS and the NI-SIS consists of:

— the network for Secure Trans-European Services for Telematics between Administrations (hereinafter referred to as 's-TESTA') that provides an encrypted, virtual, private network dedicated to SIS II data and Sirene traffic.

3. Geographical Coverage

The Communication Infrastructure must be able to cover and provide the required services to all Member States:

All EU Member States (Belgium, Czech Republic, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Slovenia, Slovakia, Finland, Sweden, United Kingdom) and Iceland, Norway, Switzerland.

In addition, coverage of the accession countries Romania and Bulgaria needs to be catered for.

Finally, the Communication Infrastructure must be able to be extended to any other country or entity acceding to the Central SIS II (e.g. Europol, Eurojust).

4. Network services

Whenever a protocol or architecture is mentioned, it should be understood that equal future technologies, protocols and architecture also are acceptable.

4.1. *Network layout*

The SIS II 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 in France and St Johann im Pongau in Austria, respectively the CS-SIS, CU and backup CS-SIS, BCU.

The central units, main and backup, must be accessible from the different Member States. The participating countries may have multiple network access points, a LNI and a BLNI, to interconnect their National System to the central services.

Apart from the main connectivity towards the central services, the Communication Infrastructure must also support bilateral supplementary information exchange between the Sirene offices of the different Member States.

4.2. *Connection type principal CS-SIS — backup CS-SIS*

The required connection type for the interconnectivity between the principal CS-SIS and the backup CS-SIS must be an SDH ring or equivalent, meaning be open also for the new future architectures and technologies. The SDH infrastructure will be used to extend the local networks of both central units to create a seamless single LAN. This LAN will then be used for the continuous synchronisation between the CU and BCU.

4.3. *Bandwidth*

A critical requirement of the Communication Infrastructure is the bandwidth size that it may grant to the different interconnected sites and its capability to support this bandwidth inside its backbone network.

The bandwidth needed for the LNI and the optional BLNI will be different for each Member State, mainly dependent on the choices of using national copies, central searching and biometric data exchange.

The actual sizes that the Communication Infrastructure decides to offer are irrelevant as long as they comply with the minimal need of each Member State.

Each of the aforementioned site types may transfer large chunks of data (alphanumeric, biometric and complete documents) in either direction. Therefore, the Communication Infrastructure must supply sufficient minimal guaranteed upload and download speeds for each connection.

The Communication Infrastructure must offer connection sizes varying from 2 Mbps up to 155 Mbps or higher. The network must supply sufficient minimal guaranteed upload and download speeds for each connection and it must be sized to support the total bandwidth size of the network access points.

4.4. *Classes of service*

The Central SIS II will support the capability of prioritisation of queries/alerts. As a derived requirement, the Communication Infrastructure will also support the possibility of traffic prioritisation.

The network prioritisation parameters are assumed to be set by the Central SIS II for all packets that require it. Weighted Fair Queuing will be used. This implies that the Communications Infrastructure must be able to take over the prioritisation assigned to the data packets on the source LAN and treat the packets accordingly within its own backbone network. Furthermore, at the remote site the Communication Infrastructure must deliver the initial packets containing the same prioritisation as set in the source LAN.

4.5. *Supported protocols*

The Central SIS II will make use of several networking communication protocols. The Communications Infrastructure should support a wide set of network communication protocols. The standard protocols to be supported are HTTP, FTP, NTP, SMTP, SNMP and DNS.

In addition to the standard protocols, the Communication Infrastructure must also be capable of handling different tunnelling protocols, SAN replication protocols and the proprietary Java-to-Java connection protocols of BEA WebLogic. The tunnelling protocols, e.g. IPsec in tunnel mode, will be used to transfer encrypted traffic to its destination.

4.6. *Technical specifications*

4.6.1. IP addressing

The Communications Infrastructure must have a range of reserved IP addresses that may solely be used within that network. Within the reserved IP range, the Central SIS II will use a dedicated set of IP addresses that will not be used anywhere else.

4.6.2. Support for IPv6

It can be assumed that the protocol used on the local networks of the Member States will be TCP/IP. However some sites will be based on version 4 while others will be based on version 6. The network access points must offer the possibility to act as a gateway and must be able to operate independently from the network protocols used in the Central SIS II as well as in the N.SIS II.

4.6.3. Static Route Injection

The CU and BCU can use a single and identical IP address for their communication to the Member States. Therefore the Communication Infrastructure should support static route injection.

4.6.4. Sustained Flow Rate

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

4.6.5. Other specifications

To support the CS-SIS, the Communication Infrastructure must at least comply with a minimum set of technical specifications:

The transit delay must 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 must 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 are to be considered for each access point separately.

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

4.7. *Resiliency*

The CS-SIS has been designed with high availability as a requirement. For this reason the system have integrated resiliency against component malfunctions by duplicating all equipment.

The components of the Communication Infrastructure must also be resilient against component failure. For the Communication Infrastructure, it means that the following components must be resilient:

— backbone network,

— routing devices,

— points of Presence,

— local loop connections (including physically redundant cabling),

— security devices (crypto devices, firewalls, etc.),

— all generic services (DNS, NTP, etc.),

— LNI/BLNI.

The failover mechanisms for all network equipment should occur without any manual intervention.

5. Monitoring

To facilitate the monitoring, the Communication Infrastructure's monitoring tools must be able to be integrated with those of the monitoring facilities of the organisation responsible for the operational management for the Central SIS II.

6. Generic services

Apart from the dedicated network and security services, the Communication Infrastructure must also offer generic services.

Dedicated services must be implemented within both central units, for redundancy purposes.

The following optional generic services must be present in the Communication Infrastructure:

Service	Additional Information
DNS	Currently the failover procedure for switching from the CU to the BCU in case of network failure is based on changing the IP address within the generic DNS server.
E-mail relay	Using a generic e-mail relay might be useful for standardising the e-mail set-up for the different Member States and, contrary to a dedicated server, does not use up any network resources from the CU/BCU. E-mails using the generic e-mail relay must still comply with their security template.
NTP	This service may be used to synchronize the clocks of network equipment.

7. Availability

The CS-SIS and the LNI and BLNI must be able to deliver an availability of 99,99 % over a 28-day rolling period excluding the network availability.

The availability of the Communication Infrastructure must be 99,99 %.

8. Security services

8.1. *Network encryption*

The Central SIS II does not allow data with high or very high protection requirements to be transferred outside the LAN without encryption. It should be ensured that the network provider will not have access to the SIS II operational data as well as to the related Sirene exchange by any means.

To maintain a high level of security, the Communication Infrastructure must allow the possibility to manage the certificates/keys. Remote administration and remote monitoring of the encryption boxes must be possible. Encryption algorithms at least must comply with the following requirements:

— symmetric encryption algorithms:

- 3DES (128 bits) or better,
- key generation must depend on random value that does not allow for key space reduction while under attack,
- encryption keys or information that can be used for deriving the keys are always protected while in storage002E;

— asymmetric encryption algorithms:

- RSA (1 024 bit modulus) or better,
- key generation must depend on random value that does not allow for key space reduction while under attack.

The Encapsulated Security Payload (ESP, RFC2406) protocol shall be used. It shall be used in tunnel mode. The Payload and the original IP-header shall be encrypted.

For exchange of session keys the Internet Key Exchange (IKE) protocol shall be used.

IKE keys shall not be valid longer than one day.

Session keys shall not be longer than one hour.

8.2. *Other security features*

Besides protecting the SIS II access points, the Communication Infrastructure must also protect the optional generic services. These services should meet the same protection measures comparable to those in CS-SIS. All generic services must therefore, at a minimum, be protected by a firewall, antivirus and an intrusion detection system. Furthermore, the generic services devices and its protection measures should be under continuous security surveillance (logging and follow-up).

In order to maintain a high level of security, the organisation responsible for the operational management for the Central SIS II must be aware of any security incidents that occur on the Communication Infrastructure. Therefore, the Communication Infrastructure must allow security incidents to be reported without any delay to the organisation responsible for the operational management for the Central SIS II. All security incidents must be provided on a regular basis, e.g. monthly reporting and ad-hoc basis.

9. **Helpdesk and support structure**

The provider of the Communication Infrastructure must deliver a helpdesk that interacts with the organisation responsible for the operational management for the Central SIS II.

10. **Interaction with other systems**

The Communication Infrastructure must ensure that information cannot go outside the assigned communication channels. For the technical implementation this implies that:

— all unauthorised and/or uncontrolled access to other networks is strictly prohibited. This includes the interconnectivity to the Internet,

— data leakage to other systems on the network may not occur; e.g. interconnection of different IP VPNs is not allowed.

Apart from the aforementioned technical restrictions it causes, it also impacts the communications infrastructure's helpdesk. The helpdesk may not release any information with regard to the Central SIS II to any party else than the one responsible for the operational management for the Central SIS II.