DECISIÓN DE LA COMISIÓN

de 16 de marzo de 2007

por la que se establecen los requisitos de la red para el Sistema de Información de Schengen II (tercer pilar)

(2007/171/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado de la Unión Europea,

Vista la Decisión 2001/886/JAI del Consejo, de 6 de diciembre de 2001, sobre el desarrollo del Sistema de Información de Schengen de segunda generación (SIS II) [1], y, en particular, su artículo 4, letra a),

Considerando lo siguiente:

(1) Para desarrollar el SIS II es necesario proponer especificaciones técnicas referentes a la red de comunicación, sus componentes y a los requisitos específicos de la red.

(2) La Comisión y los Estados miembros deben llevar a cabo los acuerdos oportunos, en especial por lo que se refiere a los elementos de la interfaz nacional uniforme situada en los Estados miembros.

(3) La presente Decisión no prejuzga la adopción en el futuro de otras decisiones de la Comisión relacionadas con el desarrollo del SIS II, en especial con el desarrollo de los requisitos de seguridad.

(4) El Reglamento (CE) nº 2424/2001 del Consejo [2] y la Decisión 2001/886/JAI rigen el desarrollo del SIS II. Para que haya un único proceso de ejecución en el desarrollo de todo el sistema SIS II, las disposiciones de la presente Decisión deben reflejar las disposiciones de la Decisión de la Comisión por la que se establecen los requisitos de red para SIS II que debe adoptarse en aplicación del Reglamento (CE) nº 2424/2001.

(5) El Reino Unido participa en la adopción de la presente Decisión de conformidad con el artículo 5 del Protocolo por el que se integra el acervo de Schengen en el marco de la Unión Europea, anejo al Tratado UE y al Tratado CE, y con el artículo 8, apartado 2, de la Decisión 2000/365/CE del Consejo, de 29 de mayo de 2000, sobre la solicitud del Reino Unido de Gran Bretaña e Irlanda del Norte de participar en algunas de las disposiciones del acervo de Schengen [3].

(6) Irlanda participa en la adopción de la presente Decisión de conformidad con el artículo 5 del Protocolo por el que se integra el acervo de Schengen en el marco de la Unión Europea, anejo al Tratado UE y al Tratado CE, y con el artículo 5, apartado 1, y el artículo 6, apartado 2, de la Decisión 2002/192/CE del Consejo, de 28 de febrero de 2002, sobre la solicitud de Irlanda de participar en algunas de las disposiciones del acervo de Schengen [4].

(7) En lo que respecta a Islandia y Noruega, la presente Decisión desarrolla las disposiciones del acervo de Schengen de conformidad con el Acuerdo celebrado por el Consejo de la Unión Europea y la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen, que entran en el ámbito a que se refiere el artículo 1, letra G, de la Decisión 1999/437/CE del Consejo [5], relativa a determinadas normas de desarrollo de dicho Acuerdo.

(8) En lo que respecta a Suiza, la presente Decisión desarrolla disposiciones del acervo de Schengen de conformidad con el Acuerdo firmado por la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen, que entran en el ámbito a que se refiere el artículo 1, letra G, de la Decisión 1999/437/CE del Consejo, en relación con el artículo 4, apartado 1, de la Decisión 2004/849/CE del Consejo [6], relativa a la firma, en nombre de la Comunidad Europea, y a la aplicación provisional de determinadas disposiciones de dicho Acuerdo.

(9) La presente Decisión constituye un acto de desarrollo del acervo de Schengen o está relacionado con este en el sentido del artículo 3, apartado 1, del Acta de adhesión.

(10) Las medidas contempladas en la presente Decisión se ajustan al dictamen del Comité establecido en virtud del artículo 5, apartado 1, de la Decisión 2001/886/JAI.

---

[1] DO L 328 de 13.12.2001, p. 1.

[2] DO L 328 de 13.12.2001, p. 4. Reglamento modificado por el Reglamento (CE) nº 1988/2006 (DO L 411 de 30.12.2006, p. 1).

[3] DO L 131 de 1.6.2000, p. 43. Decisión modificada por la Decisión 2004/926/CE (DO L 395 de 31.12.2004, p. 70).

[4] DO L 64 de 7.3.2002, p. 20.

[5] DO L 176 de 10.7.1999, p. 31.

[6] DO L 368 de 15.12.2004, p. 26.

DECIDE:

Artículo único

Las especificaciones técnicas relacionadas con el diseño de la arquitectura física de la infraestructura de comunicación del SIS II deberán ajustarse al contenido del anexo.

Hecho en Bruselas, el 16 de marzo de 2007.

Por la Comisión
Franco FRATTINI
Vicepresidente

ANEXO

ÍNDICE

1. **Introducción**

El presente documento describe el diseño de la red de comunicaciones, los componentes que la integran y los requisitos específicos de la red.

1.1. *Siglas y abreviaturas*

Esta sección describe las siglas utilizadas en el documento.

Siglas y abreviaturas	Explicación
BLNI	Interfaz nacional local de reserva
CEP	Punto final central
CNI	Interfaz nacional central
CS	Sistema central
CS-SIS	Función de apoyo técnico que contiene la base de datos SIS II
DNS	Servidor de nombres de dominio
FCIP	Canal de fibra sobre IP
FTP	Protocolo de transferencia de archivos
HTTP	Protocolo de transferencia de hipertexto
IP	Protocolo Internet
LAN	Red de área local
LNI	Interfaz nacional local
Mbps	Megabits por segundo
MDC	Contratista principal
N.SIS II	Sección nacional en cada Estado miembro
NI-SIS	Una interfaz nacional uniforme
NTP	Protocolo de sincronización de la red
SAN	Red de zona de almacenamiento
SDH	Jerarquía digital síncrona
SIS II	Sistema de información de Schengen, segunda generación
SMTP	Protocolo sencillo de transferencia de correo
SNMP (Simple Network Management Protocol)	Protocolo sencillo de gestión de redes
s-TESTA	Servicios transeuropeos seguros de telemática entre las administraciones; es una medida del programa IDABC (prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos. Decisión 2004//387/CE del Parlamento Europeo y del Consejo de 21.4.2004).
TCP	Protocolo de control de transmisiones
VIS	Sistema de información de visados
VPN	Red privada virtual
WAN	Red de área extensa

2. **Presentación general**

El SIS II se compone de:

— el sistema central (denominado en lo sucesivo «SIS II central»), que consta de:

  • una función de apoyo técnico (denominada en lo sucesivo «CS-SIS») que contiene la base de datos SIS II. La CS-SIS principal lleva a cabo la supervisión y la gestión técnicas y una CS-SIS de reserva puede realizar todas las funciones de la CS-SIS principal en caso de fallo de este sistema,

  • una interfaz nacional uniforme (denominada en lo sucesivo «NI-SIS»),

— una sección nacional (en lo sucesivo, «N.SIS II») en cada uno de los Estados miembros, compuesta por los sistemas de datos nacionales que comunican con el SIS II central. Una N.SIS II puede contener un archivo de datos (en lo sucesivo, «copia nacional»), que alberga una copia completa o parcial de la base de datos SIS II,

— una infraestructura de comunicación entre la CS-SIS y la NI-SIS (en lo sucesivo, «infraestructura de comunicación»), que provee una red virtual cifrada dedicada a los datos del SIS II y al intercambio de datos entre los servicios Sirene.

La NI-SIS consta de:

— una interfaz nacional local (en lo sucesivo, «LNI») en cada Estado miembro, que es la interfaz que conecta físicamente el Estado miembro con la red de comunicaciones segura y contiene dispositivos de cifrado dedicados al tráfico SIS II y Sirene. La LNI está situada en las instalaciones del Estado miembro,

— una interfaz nacional local de reserva, que es opcional (en lo sucesivo, «BLNI») y tiene exactamente el mismo contenido y función que la LNI.

La LNI y la BLNI son utilizadas exclusivamente por el sistema SIS II y para el intercambio Sirene. Se especificará y acordará la configuración específica de la LNI y la BLNI con cada Estado miembro para tener en cuenta los requisitos de seguridad, la localización física y las condiciones de instalación, incluida la prestación de servicios por el proveedor de red; ello supone que la conexión física s-TESTA puede contener varios túneles VPN para otros sistemas, por ejemplo, VIS y Eurodac,

— una interfaz nacional central (en lo sucesivo, «CNI») que es una aplicación que proporciona acceso a la CS-SIS. Cada Estado miembro tiene distintos puntos lógicos de acceso a la CNI a través de un cortafuegos central.

La infraestructura de comunicación entre la CS-SIS y los NI-SIS se compone de:

— la red de servicios transeuropeos seguros de telemática entre administraciones (en lo sucesivo, «s-TESTA»), que provee una red cifrada, virtual y privada dedicada a datos de SIS II y al tráfico Sirene.

3. **Cobertura geográfica**

La infraestructura de comunicación debe poder cubrir y proporcionar los servicios necesarios a todos los Estados miembros.

Esto es, todos los Estados miembros de la UE (Alemania, Austria, Bélgica, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa y Suecia), a lo que se añaden Islandia, Noruega y Suiza.

Es, además, necesario ofrecer la cobertura de los países candidatos a la adhesión, Bulgaria y Rumanía.

Por último, la infraestructura de comunicación tiene que poder ampliarse a cualquier otro país o entidad con acceso al SIS II central (por ejemplo, Europol o Eurojust).

4. **Servicios de red**

Siempre que se mencione un protocolo o una arquitectura de red, debe entenderse que son también aceptables en el futuro las tecnologías, los protocolos y la arquitectura que sean iguales.

4.1. *Diseño de la red*

La arquitectura del SIS II utiliza servicios centralizados, que son accesibles desde los diferentes Estados miembros. Por motivos de resiliencia, estos servicios centralizados se duplican en dos lugares distintos, Estrasburgo (Francia) y St Johann im Pongau (Austria), donde se encuentran, respectivamente, la unidad central (CU) y la de reserva (BCU) de la CS-SIS.

Desde los distintos Estados miembros se tiene que poder acceder a las unidades centrales, la principal y la de reserva. Los países participantes pueden tener múltiples puntos de acceso de red, una LNI y una BLNI, para interconectar su sistema nacional a los servicios centrales.

Aparte de la conectividad principal con los servicios centrales, la infraestructura de comunicación también soportará el intercambio de información complementaria bilateral entre los servicios Sirene de los distintos Estados miembros.

4.2. *Tipo de conexión entre la CS-SIS principal y la CS-SIS de reserva*

El tipo requerido de conexión para la interconectividad entre la CS-SIS principal y la CS-SIS de reserva debe ser un anillo SDH o equivalente, es decir que esté abierto también a las nuevas arquitecturas y tecnologías del futuro. Se utilizará la infraestructura SDH para ampliar las redes locales de ambas unidades centrales a fin de crear una sola LAN, que se utilizará después para la sincronización continua entre la CU y la BCU.

4.3. *Ancho de banda*

Un requisito importante de la infraestructura de comunicación es la dimensión del ancho de banda que puede ofrecer a los distintos sitios interconectados y su capacidad de soportar este ancho de banda dentro de su red básica.

Cada Estado miembro necesitará un ancho de banda distinto para la LNI y la BLNI opcional, y ello dependerá esencialmente de la decisión de utilizar copias nacionales, búsqueda central e intercambio de datos biométricos.

Es irrelevante la dimensión real que la infraestructura de comunicación decida ofrecer, siempre y cuando cumpla con las necesidades mínimas de cada Estado miembro.

Cada uno de los tipos de sitios antes mencionados puede transferir segmentos grandes de datos (alfanuméricos, biométricos y documentos completos) en ambas direcciones. Es, por lo tanto, necesario que la infraestructura de comunicación suministre unas velocidades mínimas garantizadas de carga y descarga suficientes para cada conexión.

La infraestructura de comunicación debe ofrecer dimensiones de conexión que oscilen entre 2 Mbps y 155 Mbps o superiores. La red tiene que suministrar unas velocidades mínimas garantizadas de carga y descarga suficientes para cada conexión y tener unas dimensiones que soporten el tamaño total de ancho de banda de los puntos de acceso de red.

4.4. *Tipos de servicios*

El SIS II central soportará la capacidad de priorización de consultas/alertas. Como requisito derivado, la infraestructura de comunicación soportará también la posibilidad de establecer prioridades en el tráfico.

El SIS II central tendrá que fijar los parámetros de priorización de red para todos los paquetes de datos que lo requieren. Se utilizará el sistema WFQ (espera equitativa ponderada), lo que significa que la infraestructura de comunicación tiene que poder asumir la priorización asignada a los paquetes de datos en la LAN de origen y procesarlos en consonancia en su propia red básica. Además, en el sitio remoto la infraestructura de comunicación debe respetar la misma priorización establecida en la LAN de origen en la entrega de los paquetes iniciales.

4.5. *Protocolos*

El SIS II central hará uso de varios protocolos de comunicación en redes. La infraestructura de comunicación debe soportar una amplia serie de protocolos de comunicación, entre los que están los protocolos estándar HTTP, FTP, NTP, SMTP, SNMP y DNS.

Además de estos protocolos estándar, la infraestructura de comunicación debe también ser capaz de manejar diversos protocolos de tunelización, los protocolos de reproducción SAN y los protocolos de conexión de Java a Java propiedad del proveedor BEA WebLogic. Para transferir el tráfico cifrado a su destino se utilizarán protocolos de tunelización, por ejemplo IPsec en modo túnel.

4.6. *Especificaciones técnicas*

4.6.1. Direcciones IP

La infraestructura de comunicación tiene que contar con una gama de direcciones IP reservadas, de uso exclusivo dentro de dicha red. En la gama reservada IP, el SIS II central utilizará un grupo dedicado de direcciones IP que no se utilizará en ninguna otra parte.

4.6.2. Soporte de IPv6

Cabe pensar que el protocolo utilizado en las redes locales de los Estados miembros será TCP/IP; algunos sitios, no obstante, utilizarán la versión 4 y otros la versión 6. Es importante que los puntos de acceso a la red puedan actuar de pasarela y funcionen con independencia de los protocolos de red utilizados en el SIS II central y en el N.SIS II.

4.6.3. Inyección de rutas estáticas

La unidad central y la de reserva pueden utilizar la misma dirección IP para su comunicación con los Estados miembros. Por lo tanto, la infraestructura de comunicación debe soportar la inyección de rutas estáticas.

4.6.4. Velocidad sostenida

Siempre y cuando la conexión de la unidad central o la de reserva tenga un índice de carga inferior al 90 %, un Estado miembro determinado debe poder soportar continuamente el 100 % de su ancho de banda especificado.

4.6.5. Otras especificaciones

Para soportar la CS-SIS, la infraestructura de comunicación debe cumplir por lo menos con un grupo mínimo de especificaciones técnicas:

El retardo de tránsito debe ser (incluidas las horas punta) inferior o igual a 150 ms en el 95 % de los paquetes e inferior a 200 ms en el 100 % de los paquetes.

La probabilidad de pérdida de paquete debe ser (incluidas las horas punta) inferior o igual a 10^{-4} en el 95 % de los paquetes e inferior a 10^{-3} en el 100 % de los paquetes.

Las especificaciones mencionadas anteriormente tienen que ser tenidas en cuenta en cada punto de acceso separadamente.

La conexión entre la unidad central y la de reserva debe tener un tiempo de retardo de ida y vuelta inferior o igual a 60 ms.

4.7. *Resiliencia*

Como la CS-SIS ha sido concebida para ofrecer una gran disponibilidad, el sistema ha incorporado, mediante la duplicación de todos sus equipos, la resiliencia contra el mal funcionamiento de sus componentes.

Los componentes de la infraestructura de comunicación deben ser también resistentes contra el fallo de uno de ellos. En la infraestructura de comunicación, deben ser resistentes los siguientes componentes:

— la red básica,

— los dispositivos de encaminamiento,

— los puntos de presencia,

— las conexiones de bucle local (incluido el cableado físicamente redundante),

— los dispositivos de seguridad (dispositivos de cifrado, cortafuegos, etc.),

— todos los servicios genéricos (DNS, NTP, etc.),

— la LNI/BLNI.

Los mecanismos de traspaso en caso de avería de todos los equipos de la red deben funcionar sin intervención manual.

5. **Supervisión**

Para facilitar la supervisión, deben poder integrarse los instrumentos de la infraestructura de comunicación a tal efecto con los dispositivos correspondientes de la organización responsable de la gestión operativa del SIS II central.

6. **Servicios genéricos**

Aparte de los servicios dedicados de red y seguridad, la infraestructura de comunicación también tiene que ofrecer servicios genéricos.

Habrá que poner en marcha servicios dedicados en ambas unidades centrales, por motivos de redundancia.

En la infraestructura de comunicación, deben estar presentes los siguientes servicios genéricos opcionales:

Servicio	Información adicional
DNS	Actualmente el procedimiento de traspaso entre la CU y la BCU en caso de fallo de la red se basa en el cambio de la dirección IP en el servidor genérico DNS.
Retransmisor de correo electrónico	La utilización de un retransmisor genérico de correo electrónico podría ser útil para estandarizar la configuración del correo electrónico en los distintos Estados miembros y, al contrario que un servidor dedicado, no consume recursos de red de la CU/BCU. Los correos electrónicos que utilizan el retransmisor genérico de correo electrónico tienen que aplicar además su plantilla de seguridad.
NTP	Puede utilizarse este servicio para sincronizar los relojes de los equipos de red.

7. **Disponibilidad**

La CS-SIS, la LNI y la BLNI tienen que presentar una disponibilidad del 99,99 % a lo largo de un período rotatorio de 28 días, excluida la disponibilidad de la red.

La disponibilidad de la infraestructura de comunicación debe ser del 99,99 %.

8. **Servicios de seguridad**

8.1. *Cifrado de red*

El SIS II central no permite que se transfieran datos con requisitos altos o muy altos de protección fuera de la LAN si no aparecen cifrados. Habrá que garantizar que el proveedor de red no tiene en absoluto acceso a los datos operativos del SIS II ni al correspondiente intercambio Sirene.

Para mantener un alto nivel de seguridad, la infraestructura de comunicación debe permitir gestionar los certificados/las claves, haciendo posibles la administración y el control remotos de las cajas de cifrado. Los algoritmos del cifrado deben cumplir por lo menos los siguientes requisitos:

— Algoritmos simétricos de cifrado:

• 3DES (128 bits) o superior,

• la generación de las claves debe depender de un valor aleatorio que no permita la reducción de espacio de claves si se produce un ataque,

• las claves del cifrado o la información que puede servir para deducir las claves están protegidas incluso cuando están almacenadas.

— Algoritmos asimétricos de cifrado:

• RSA (módulo de 1 024 bits) o superior,

• la generación de las claves debe depender de un valor aleatorio que no permita la reducción del espacio de claves si se produce un ataque.

Se utilizará el protocolo de carga de seguridad encapsulada (ESP, RFC2406), en modo túnel. Aparecerán cifrados la carga útil y el encabezamiento IP original.

Para el intercambio de claves de sesión se recurrirá al protocolo de intercambio de claves de Internet (IKE).

La validez de las claves IKE no será superior a un día.

Las claves de sesión no durarán más de una hora.

8.2. *Otras características de seguridad*

Además de proteger los puntos de acceso de SIS II, la infraestructura de comunicación debe también proteger los servicios genéricos opcionales, que tienen que cumplir medidas de seguridad comparables a las de la CS-SIS. Por ello, todos los servicios genéricos deben, como mínimo, estar protegidos por un cortafuegos, un antivirus y un sistema de detección de la intrusión. Además, sería conveniente que estos dispositivos y sus medidas de protección estuvieran sometidos a vigilancia continua de seguridad (registro y seguimiento).

Para mantener un alto nivel de seguridad, se debe informar a la organización responsable de la gestión operativa del SIS II central de cualquier incidente relacionado con la seguridad que ocurra en la infraestructura de comunicación. Por lo tanto, esta infraestructura debe hacer posible una rápida información de todos los incidentes importantes en materia de seguridad a la organización responsable de la gestión operativa del SIS II central. Sería deseable que se comunicaran todos los incidentes de seguridad regularmente, por ejemplo mensualmente y sobre una base *ad hoc*.

9. **Servicio de asistencia y apoyo**

El proveedor de la infraestructura de comunicación debe prestar un servicio de asistencia que interactúe con la organización responsable de la gestión operativa del SIS II central.

10. **Interacción con otros sistemas**

La infraestructura de comunicación debe garantizar que la información no pueda salir de los canales de comunicación asignados. En la aplicación técnica esto significa que:

— estará estrictamente prohibido el acceso no autorizado e incontrolado a otras redes, incluida la interconectividad con Internet,

— no será posible el filtrado de datos a otros sistemas en la red; por ejemplo no se permitirá la interconexión de distintas redes privadas virtuales (VPN) con IP.

Aparte de las restricciones técnicas antes mencionadas que origina, también afecta al servicio de asistencia de la infraestructura de comunicación, que no podrá dar a conocer ninguna información referente al SIS II central a ningún otro agente excepto al responsable de la gestión operativa del SIS II central.