DÉCISION DE LA COMMISSION

du 16 mars 2007

établissant les caractéristiques du réseau du système d'information Schengen II (3e pilier)

(2007/171/CE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité sur l'Union européenne,

vu la décision 2001/886/JAI du Conseil du 6 décembre 2001 relative au développement du système d'information de Schengen de deuxième génération (SIS II) [1], et notamment son article 4, point a),

considérant ce qui suit:

(1) Pour développer le SIS II, il y a lieu de définir des caractéristiques techniques relatives au réseau de communication et à ses composants, et de déterminer les exigences spécifiques liées au réseau.

(2) Il y a lieu de fixer des modalités appropriées entre la Commission et les États membres, notamment en ce qui concerne les éléments de l'interface nationale uniforme située dans les États membres.

(3) La présente décision ne porte pas atteinte à l'adoption ultérieure d'autres décisions de la Commission concernant le développement du SIS II, notamment sur la définition des exigences en matière de sécurité.

(4) Tant le règlement (CE) nº 2424/2001 du Conseil [2] que la décision 2001/886/JAI régissent le développement du SIS II. Pour garantir que le développement du SIS II dans son ensemble ne fasse l'objet que d'un seul et même processus de mise en œuvre, les dispositions de la présente décision doivent correspondre à celles de la décision de la Commission établissant les caractéristiques du réseau du SIS II qui doit être adoptée en application du règlement (CE) nº 2424/2001.

(5) Le Royaume-Uni participe à la présente décision, conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne, annexé au traité UE et au traité CE, et conformément à l'article 8, paragraphe 2, de la décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen [3].

(6) L'Irlande participe à la présente décision, conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne, annexé au traité UE et au traité CE, et conformément à l'article 5, paragraphe 1, et à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen [4].

(7) En ce qui concerne l'Islande et la Norvège, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, qui relève du domaine visé à l'article 1er, point G, de la décision 1999/437/CE du Conseil [5] relative à certaines modalités d'application de cet accord.

(8) En ce qui concerne la Suisse, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, qui relève du domaine visé à l'article 1er, point G, de la décision 1999/437/CE en liaison avec l'article 4, paragraphe 1, de la décision 2004/849/CE du Conseil [6] relative à la signature, au nom de l'Union européenne, et à l'application provisoire de certaines dispositions de cet accord.

(9) La présente décision constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte au sens de l'article 3, paragraphe 1, de l'acte d'adhésion.

(10) Les mesures prévues dans la présente décision sont conformes à l'avis du comité créé en vertu de l'article 5, paragraphe 1, de la décision 2001/886/JAI,

[1] JO L 328 du 13.12.2001, p. 1.
[2] JO L 328 du 13.12.2001, p. 4. Règlement modifié par le règlement (CE) nº 1988/2006 (JO L 411 du 30.12.2006, p. 1).
[3] JO L 131 du 1.6.2000, p. 43. Décision modifiée par la décision 2004/926/CE (JO L 395 du 31.12.2004, p. 70).
[4] JO L 64 du 7.3.2002, p. 20.
[5] JO L 176 du 10.7.1999, p. 31.
[6] JO L 368 du 15.12.2004, p. 26.

DÉCIDE:

Article unique

Les caractéristiques techniques relatives à la conception de l'architecture physique de l'infrastructure de communication du SIS II sont exposées en annexe.

Fait à Bruxelles, le 16 mars 2007.

Par la Commission
Franco FRATTINI
Vice-président

ANNEXE

TABLE DES MATIÈRES

1. **Introduction**

Le présent document décrit la conception du réseau de communication, ses composants ainsi que les exigences propres au réseau.

1.1. *Acronymes et abréviations*

La présente section explique les acronymes utilisés dans l'ensemble du document.

Acronymes et abréviations	Explication
BLNI	Interface nationale locale de secours
CEP	Central End Point
CNI	Interface nationale centrale
CS	Système central
CS-SIS	Fonction de support technique contenant la base de données SIS II
DNS	Serveur de nom de domaine
FCIP	Fibre Channel sur IP
FTP	Protocole de transfert de fichier
HTTP	Protocole de transfert d'hypertexte
IP	Protocole internet
LAN	Réseau local
LNI	Interface nationale locale
Mbps	Mégabits par seconde
MDC	Main Developer Contractor
N.SIS II	Section nationale dans chaque État membre
NI-SIS	Interface nationale uniforme
NTP	Protocole de synchronisation réseau
SAN	Réseau de stockage
SDH	Hiérarchie numérique synchrone
SIS II	Système d'information de Schengen, deuxième génération
SMTP	Protocole de transfert de courrier simple
SNMP	Protocole de gestion de réseau simple
s-TESTA	Services télématiques transeuropéens sécurisés entre administrations, relevant du programme IDABC (fourniture interopérable de services paneuropéens de gouvernement électronique aux administrations publiques, aux entreprises et aux citoyens. Décision 2004/387/CE du Parlement européen et du Conseil du 21.4.2004).
TCP	Protocole de contrôle de transmission
VIS	Système d'information sur les visas
VPN	Réseau privé virtuel
WAN	Réseau longue distance

2. **Vue d'ensemble**

Le SIS II se compose:

— d'un système central (ci-après dénommé «SIS II central») comprenant:

  • une fonction de support technique (ci-après dénommée «CS-SIS») contenant la base de données SIS II. Le système central principal du CS-SIS assure le contrôle et la gestion, et un système central de secours est capable d'assurer l'ensemble des fonctionnalités du système central principal en cas de défaillance de celui-ci;

  • une interface nationale uniforme (ci-après dénommée «NI-SIS»);

— d'une section nationale (ci-après dénommée «N.SIS II») dans chaque État membre, constituée des systèmes de données nationaux reliés au SIS II central. Une section N.SIS II peut contenir un fichier de données (ci-après dénommé «copie nationale»), qui comporte une copie complète ou partielle de la base de données SIS II;

— d'une infrastructure de communication entre le CS-SIS et les NI-SIS (ci-après dénommée «infrastructure de communication») qui assure des communications par réseau virtuel et crypté, affecté aux données du SIS II et aux échanges de données entre les bureaux SIRENE.

Les NI-SIS se composent:

— d'une interface nationale locale (ci-après dénommée «LNI») dans chaque État membre, c'est-à-dire l'interface qui établit la connexion physique entre l'État membre et le réseau de communication sécurisé et qui contient les dispositifs de cryptage affectés au trafic du SIS II et du réseau SIRENE. La LNI est située dans l'État membre;

— d'une interface nationale locale de secours facultative (ci-après dénommée «BLNI») dont le contenu et la fonction sont identiques à ceux de la LNI.

La LNI et la BLNI sont utilisées exclusivement par le SIS II et pour les échanges SIRENE. La configuration spécifique de la LNI et celle de la BLNI seront spécifiées et convenues avec chaque État membre, afin de tenir compte des exigences de sécurité, de l'emplacement physique et des conditions d'installation de ces interfaces, ainsi que la prestation de services par le fournisseur du réseau, de sorte que la connexion s-TESTA physique puisse englober plusieurs tunnels VPN pour d'autres systèmes, par exemple le VIS et Eurodac;

— d'une interface nationale centrale (ci-après dénommée «CNI») qui est une application qui sécurise l'accès au CS-SIS. Chaque État membre dispose de points logiques distincts pour accéder à la CNI via un pare-feu central.

L'infrastructure de communication entre le CS-SIS et les NI-SIS se compose:

— du réseau de services télématiques transeuropéens sécurisés entre administrations (ci-après dénommé «s-TESTA») qui garantit des communications par réseau crypté, virtuel et privé affecté aux données du SIS II et au trafic SIRENE.

3. **Couverture géographique**

L'infrastructure de communication doit pouvoir englober et fournir à tous les États membres les services requis.

Sont concernés tous les États membres de l'Union européenne (Belgique, France, Allemagne, Luxembourg, Pays-Bas, Italie, Portugal, Espagne, Grèce, Autriche, Danemark, Finlande, Suède, Chypre, République tchèque, Estonie, Hongrie, Lettonie, Lituanie, Malte, Pologne, Slovaquie, Slovénie, Royaume-Uni et Irlande), ainsi que la Norvège, l'Islande et la Suisse.

Il y a également lieu de prévoir la couverture des pays qui viennent d'adhérer, à savoir la Roumanie et la Bulgarie.

Enfin, l'infrastructure de communication doit pouvoir être étendue à tout autre pays ou entité susceptible d'avoir accès au SIS II central (par exemple, Europol ou Eurojust).

4. **Services du réseau**

Lorsqu'il est fait mention d'un protocole ou d'une architecture, il est entendu que des technologies, protocoles et architectures équivalents à venir seront également admis.

4.1. *Structure du réseau*

L'architecture du SIS II repose sur des services centralisés, qui sont accessibles depuis les États membres. Pour des questions de résilience, ces services centralisés sont dupliqués dans deux sites, à savoir Strasbourg en France et St Johann im Pongau en Autriche, où se trouvent respectivement l'unité principale (CU) et l'unité de secours (BCU) du CS-SIS.

Les unités centrales — principale et de secours — doivent être accessibles depuis les États membres. Les pays participants peuvent disposer de plusieurs points d'accès au réseau, d'une LNI et d'une BLNI, pour relier leur système national aux services centraux.

Outre la connectivité générale avec les services centraux, l'infrastructure de communication doit également assurer les échanges bilatéraux d'informations supplémentaires entre les bureaux SIRENE des États membres.

4.2. *Type de connexion entre le CS-SIS principal et le CS-SIS de secours*

Le type de connexion requis pour l'interconnectivité entre le CS-SIS principal et le CS-SIS de secours est une boucle SDH ou un équivalent, c'est-à-dire que la connexion doit être possible à l'avenir avec des architectures ou des technologies nouvelles. Il sera recouru à l'infrastructure SDH pour élargir les réseaux locaux des deux unités centrales, afin de créer un LAN unique sans rupture. Ce LAN servira ensuite à la synchronisation continue entre l'unité centrale principale et l'unité centrale de secours.

4.3. *Bande passante*

Une exigence essentielle de l'infrastructure de communication est la largeur de la bande passante que celle-ci sera en mesure d'accorder aux différents sites interconnectés et sa capacité à supporter cette bande passante au sein de son réseau fédérateur.

La bande passante nécessaire à la LNI et à la BLNI facultative variera d'un État membre à l'autre, essentiellement selon que celui-ci choisira de recourir ou non à des copies nationales, à la fonction de recherche centrale et à l'échange de données biométriques.

La largeur réelle que l'infrastructure de communication offrira est sans importance pour autant qu'elle réponde aux besoins minimaux de chaque État membre.

Chacun des types de site susmentionnés pourra transférer de volumineux datagrammes (données alphanumériques, biométriques, ainsi que des documents entiers) dans l'un ou l'autre sens. C'est pourquoi l'infrastructure de communication doit offrir et garantir des vitesses de téléchargement minimales suffisantes lors de chaque connexion.

L'infrastructure de communication doit assurer un débit de connexion allant de 2 Mbps à 155 Mbps, voire plus. Le réseau doit offrir et garantir des vitesses de téléchargement minimales suffisantes lors de chaque connexion et il doit être capable de supporter la largeur globale de la bande passante des points d'accès au réseau.

4.4. *Catégories de services*

Le SIS II central sera en mesure de traiter, selon un ordre de priorité, les interrogations et les signalements. Par conséquent, l'infrastructure de communication devra également assurer la gestion du trafic par ordre de priorité.

Les paramètres permettant d'établir les priorités du réseau sont censés être fixés par le SIS II central pour tous les datagrammes qui l'exigent. La gestion des datagrammes en attente sera assurée par le mécanisme «*Weighted Fair Queuing*». Cela implique que l'infrastructure de communication doit être capable de reprendre l'ordre de priorité attribué aux datagrammes dans le LAN source et de traiter ceux-ci selon cet ordre au sein de son réseau fédérateur. En outre, elle doit transmettre au site distant les datagrammes initiaux contenant le même ordre de priorité que celui fixé dans le LAN source.

4.5. *Protocoles supportés*

Le SIS II central fera appel à plusieurs protocoles de communication en réseau et l'infrastructure de communication devra supporter une large gamme de ceux-ci. Les protocoles standard qui devront être supportés sont HTTP, FTP, NTP, SMTP, SNMP et DNS.

Outre ceux-ci, l'infrastructure de communication doit aussi être capable de gérer différents protocoles d'acheminement, des protocoles de duplication SAN et les protocoles propriétaires de connexion «Java to Java» de BEA WebLogic. Les protocoles d'acheminement, par exemple IPsec en mode tunnel, seront utilisés pour amener des messages cryptés à leur destination.

4.6. *Caractéristiques techniques*

4.6.1. Adressage IP

L'infrastructure de communication doit disposer d'une gamme d'adresses IP réservées ne pouvant être utilisées qu'au sein de ce réseau. Dans cette gamme réservée, le SIS II central n'utilisera qu'une série unique d'adresses IP qui ne seront pas employées ailleurs.

4.6.2. Support pour IPv6

L'on peut supposer que le protocole qui sera utilisé sur les réseaux locaux des États membres sera le TCP/IP. Certains sites recourront toutefois à la version 4 tandis que d'autres fonctionneront avec la version 6. Les points d'accès au réseau doivent pouvoir faire office de portail et être capables de fonctionner indépendamment des protocoles de réseau utilisés dans le SIS II central ainsi que dans les N.SIS II.

4.6.3. Routage statique

L'unité principale et l'unité de secours peuvent utiliser une même adresse IP pour leurs communications destinées aux États membres. L'infrastructure de communication doit donc permettre un routage statique.

4.6.4. Débit soutenu

Tant que l'unité principale ou l'unité de secours affiche un taux de charge inférieur à 90 %, un État membre donné doit pouvoir maintenir en permanence 100 % de sa bande passante.

4.6.5. Autres caractéristiques techniques

Pour supporter le CS-SIS, l'infrastructure de communication doit être conforme à une série minimale de caractéristiques techniques.

Le délai de transit doit (y compris pendant les heures de pointe) être inférieur ou égal à 150 ms pour 95 % des datagrammes et inférieur à 200 ms pour 100 % des datagrammes.

La probabilité de perte de datagramme doit (y compris durant les heures de pointe) être inférieure ou égale à 10^{-4} pour 95 % des datagrammes et inférieure à 10^{-3} pour 100 % des datagrammes.

Les caractéristiques techniques susmentionnées doivent s'appliquer à chacun des points d'accès.

La connexion entre l'unité principale et l'unité de secours doit comporter un temps de transmission aller-retour inférieur ou égal à 60 ms.

4.7. *Résilience*

Le CS-SIS a été conçu de manière à répondre à l'exigence d'un degré élevé de disponibilité. C'est pourquoi le système offre une résilience intégrée contre les défaillances de ses composants, grâce à la duplication de tous les équipements.

Les composants de l'infrastructure de communication doivent aussi résister aux failles de l'un d'entre eux. Cela signifie que les composants suivants doivent tolérer les pannes:

— le réseau fédérateur,

— les dispositifs de routage,

— les points de présence,

— les connexions à la boucle locale (y compris le câblage redondant),

— les dispositifs de sécurité (dispositifs de cryptage, pare-feu, etc.),

— tous les services génériques (DNS, NTP, etc.),

— la LNI/BLNI.

Les mécanismes de relais en cas de panne pour tous les équipements du réseau doivent fonctionner sans intervention manuelle.

5. **Surveillance**

Pour faciliter la surveillance, les outils de surveillance de l'infrastructure de communication doivent pouvoir s'intégrer aux dispositifs de surveillance de l'organisation responsable de la gestion opérationnelle du SIS II central.

6. **Services génériques**

Outre le réseau spécialisé et les services de sécurité, l'infrastructure de communication doit également offrir des services génériques.

Des services spécialisés doivent être mis en œuvre dans les deux unités centrales, à des fins de redondance.

L'infrastructure de communication doit offrir les services génériques facultatifs suivants:

Service	Informations supplémentaires
DNS	Actuellement, la procédure de relais qui permet de basculer de l'unité principale vers l'unité de secours en cas de défaillance du réseau repose sur un changement d'adresse IP au sein du serveur DNS générique.
Relais du courrier électronique	Le recours à un relais de courrier électronique générique pourrait s'avérer utile pour standardiser l'installation des différents États membres et, contrairement à un serveur dédié, il ne consommerait pas les ressources réseau des unités principale et de secours. Les courriers électroniques passant par le relais générique doivent cependant être conformes à leur modèle de sécurité. Les courriers électroniques passant par le relais générique doivent cependant être conformes à leur modèle de sécurité.
NTP	Ce service peut être utilisé pour synchroniser les horloges des équipements du réseau.

7. **Disponibilité**

Le CS-SIS ainsi que la LNI et la BLNI doivent être capables d'offrir une disponibilité de 99,99 % sur une période continue de vingt-huit jours, indépendamment de la disponibilité du réseau.

La disponibilité de l'infrastructure de communication doit être de 99,99 %.

8. **Services de sécurité**

8.1. *Cryptage du réseau*

Le SIS II central ne permet pas le transfert non crypté en dehors du LAN de données assorties d'une exigence de protection élevée ou très élevée. Il y a lieu de s'assurer que le fournisseur du réseau n'aura aucunement accès aux données opérationnelles du SIS II ni aux échanges SIRENE connexes.

Pour maintenir un niveau élevé de sécurité, l'infrastructure de communication doit permettre la gestion de certificats/clés. La gestion et la surveillance à distance des boîtiers de chiffrement doivent être possibles. Les algorithmes de chiffrement doivent au minimum satisfaire aux exigences suivantes:

— Algorithmes de chiffrement symétrique:

  • 3DES (128 bits) ou mieux,

  • la génération de clés doit dépendre d'une valeur aléatoire qui ne permette pas la réduction de l'espace de clé en cas d'attaque,

  • les clés ou les informations de chiffrement susceptibles d'être utilisées pour dériver les clés sont toujours protégées durant leur stockage.

— Algorithmes de chiffrement asymétrique:

  • RSA (module 1 024 bits) ou mieux,

  • la génération de clés doit dépendre d'une valeur aléatoire qui ne permette pas la réduction de l'espace de clé en cas d'attaque.

Le protocole d'encapsulation de la charge utile de sécurité (ESP, RFC2406) sera utilisé en mode tunnel. La charge utile et l'entête IP d'origine feront l'objet d'un chiffrement.

Le protocole d'échange de clés internet (IKE) sera utilisé pour échanger des clés de session.

La validité des clés IKE ne dépassera pas un jour.

Les clés de session ne dureront pas plus d'une heure.

8.2. *Autres dispositifs de sécurité*

Outre qu'elle doit préserver les points d'accès au SIS II, l'infrastructure de communication doit protéger les services génériques facultatifs. Ceux-ci doivent faire l'objet de mesures de protection comparables à celles qui s'appliquent au CS-SIS. Tous les services génériques doivent donc, au minimum, être protégés par un pare-feu, un antivirus et un système de détection d'intrusion. Par ailleurs, les dispositifs liés aux services génériques et les mesures de protection qui s'y rapportent doivent faire l'objet d'une surveillance permanente (journalisation et suivi).

Pour maintenir un degré élevé de sécurité, l'organisation responsable de la gestion opérationnelle du SIS II central doit être informée de tous les incidents de sécurité qui surviennent dans l'infrastructure de communication. L'infrastructure de communication doit donc permettre la notification rapide des incidents de sécurité à l'organisation responsable de la gestion opérationnelle du SIS II central. Tous les incidents de sécurité doivent être signalés régulièrement, par exemple par des rapports mensuels et ponctuels.

9. **Service d'assistance et structure d'appui**

Le fournisseur de l'infrastructure de communication doit offrir un service d'assistance qui est en liaison étroite avec l'organisation responsable de la gestion opérationnelle du SIS II central.

10. **Interaction avec d'autres systèmes**

L'infrastructure de communication doit empêcher que des informations sortent des canaux de communication qui leur sont assignés. Sous l'angle de la mise en œuvre technique, cela implique que:

— tout accès non autorisé et/ou non contrôlé à d'autres réseaux est strictement interdit; cela vaut aussi pour l'interconnectivité avec l'internet,

— les fuites organisées de données vers d'autres systèmes sur le réseau ne peuvent se produire; par exemple, l'interconnexion de différents VPN IP n'est pas permise.

Outre les restrictions techniques susmentionnées qu'elle comporte, l'infrastructure de communication a aussi des répercussions sur le service d'assistance. Celui-ci ne peut divulguer des informations relatives au SIS II central à aucune autre entité que l'organisation responsable de la gestion opérationnelle de ce système.