DECIZIA COMISIEI

din 16 martie 2007

de stabilire a cerințelor rețelei Sistemului de Informații Schengen din a doua generație – SIS II (al treilea pilon)

(2007/171/CE)

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul privind Uniunea Europeană,

având în vedere Decizia 2001/886/JAI a Consiliului din 6 decembrie 2001 privind dezvoltarea Sistemului de Informații Schengen din a doua generație (SIS II) [1], în special articolul 4 litera (a),

întrucât:

(1) Pentru a dezvolta SIS II este necesar să se determine caracteristicile tehnice ale rețelei de comunicații, componentele sale și normele specifice ale rețelei.

(2) Trebuie stabilite modalități adecvate, în special cu privire la elementele interfeței naționale uniforme situate în statele membre, de către Comisie și statele membre.

(3) Prezenta decizie nu aduce atingere adoptării deciziilor viitoare ale Comisiei privind dezvoltarea SIS II, în special privind stabilirea normelor de securitate.

(4) Dezvoltarea SIS II este reglementată atât prin Regulamentul (CE) nr. 2424/2001 al Consiliului [2], cât și prin Decizia 2001/886/JAI. Pentru a garanta o punere în aplicare unică a procesului de dezvoltare a SIS II în ansamblul său, dispozițiile prezentei decizii trebuie să reflecteze dispozițiile Deciziei Comisiei de stabilire a cerințelor rețelei SIS II, care trebuie aplicată conform Regulamentului (CE) nr. 2424/2001.

(5) Regatul Unit ia parte la prezenta decizie în conformitate cu articolul 5 din protocolul care integrează acquis-ul Schengen în cadrul Uniunii Europene, anexat la Tratatul UE și la Tratatul CE, și cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului din 29 mai 2000 privind solicitarea Regatului Unit al Marii Britanii și Irlandei de Nord de a participa la unele dintre dispozițiile acquis-ului Schengen [3].

(6) Irlanda ia parte la această decizie în conformitate cu articolul 5 din protocolul care integrează acquis-ul Schengen în cadrul Uniunii Europene, anexat la Tratatul UE și la Tratatul CE, și cu articolul 5 alineatul (1) și articolul 6 alineatul (2) din Decizia 2002/192/CE a Consiliului din 28 februarie 2002 privind solicitarea Irlandei de a participa la unele dintre dispozițiile acquis-ului Schengen [4].

(7) În ceea ce privește Islanda și Norvegia, prezenta decizie constituie o evoluție a dispozițiilor acquis-ului Schengen în sensul acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei cu privire la asocierea acestor două state în vederea punerii în aplicare, a asigurării respectării și dezvoltării acquis-ului Schengen, care intră în sfera de aplicare a articolului 1 litera G din Decizia 1999/437/CE a Consiliului [5] privind anumite norme de aplicare a acestui acord.

(8) În ceea ce privește Elveția, prezenta decizie constituie o evoluție a dispozițiilor acquis-ului Schengen în sensul acordului încheiat de Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene în vederea punerii în aplicare, a asigurării respectării și dezvoltării acquis-ului Schengen, care intră în sfera de aplicare a articolului 1 litera G din Decizia 1999/437/CE a Consiliului coroborat cu articolul 4 alineatul (1) din Decizia 2004/849/CE a Consiliului [6] privind semnarea, în numele Uniunii Europene, și aplicarea provizorie a anumitor dispoziții ale acestui acord.

(9) Prezenta decizie constituie un act întemeiat pe acquis-ul Schengen sau care se referă la acesta în sensul articolului 3 alineatul (1) din Actul de aderare.

(10) Măsurile prevăzute de prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 5 alineatul (1) din Decizia 2001/886/JAI,

[1] JO L 328, 13.12.2001, p. 1.
[2] JO L 328, 13.12.2001, p. 4. Regulament, astfel cum a fost modificat prin Regulamentul (CE) nr. 1988/2006 (JO L 411, 30.12.2006, p. 1).
[3] JO L 131, 1.6.2000, p. 43. Decizie, astfel cum a fost modificat prin Decizia 2004/926/CE (JO L 395, 31.12.2004, p. 70).
[4] JO L 64, 7.3.2002, p. 20.
[5] JO L 176, 10.7.1999, p. 31.
[6] JO L 368, 15.12.2004, p. 26.

DECIDE:

Articol unic

Caracteristicile tehnice privind conceperea arhitecturii fizice a infrastructurii de comunicații a SIS II sunt cele stabilite în anexă.

Adoptată la Bruxelles, 16 martie 2007.

Pentru Comisie
Franco FRATTINI
Vicepreședinte

ANEXĂ

CUPRINS

1. Introducere ... 32
1.1. Acronime și abrevieri ... 32
2. Privire de ansamblu ... 33
3. Acoperire geografică ... 33
4. Servicii de rețea ... 34
4.1. Structura rețelei ... 34
4.2. Tip de conexiune între CS-SIS principal și CS-SIS de siguranță ... 34
4.3. Lățimea de bandă ... 34
4.4. Categorii de servicii ... 34
4.5. Protocoale suportate ... 35
4.6. Caracteristici tehnice ... 35
4.6.1. Adresare IP ... 35
4.6.2. Suport pentru IPv6 ... 35
4.6.3. Routare statică ... 35
4.6.4. Debit susținut ... 35
4.6.5. Alte caracteristici ... 35
4.7. Rezistență ... 35
5. Monitorizare ... 36
6. Servicii generice ... 36
7. Disponibilitate ... 36
8. Servicii de siguranță ... 36
8.1. Criptarea rețelei ... 36
8.2. Alte dispoziții de siguranță ... 37
9. Asistență și structură de sprijin ... 37
10. Interacțiunea cu alte sisteme ... 37

1. **Introducere**

Prezentul document descrie arhitectura rețelei de comunicații, componentele sale și cerințele specifice rețelei.

1.1. *Acronime și abrevieri*

Prezenta secțiune descrie acronimele utilizate în document.

Acronime și abrevieri	Explicație
BLNI	Interfață națională locală de rezervă (Backup Local National Interface)
CEP	Punct final central (Central End Point)
CNI	Interfață națională centrală (Central National Interface)
CS	Sistem central (Central System)
CS-SIS	Funcție de suport tehnic care conține baza de date SIS II
DNS	Server nume de domeniu (Domain Name Server)
FCIP	Canal de fibre pe IP (Fibre Channel over IP)
FTP	Protocol de transfer de fișiere (File Transport Protocol)
HTTP	Protocol de transfer hipertext (Hyper Text Transfer Protocol)
IP	Protocol internet (Internet Protocol)
LAN	Rețea locală (Local Area Network)
LNI	Interfață națională locală (Local National Interface)
Mbps	Megabiți pe secundă
MDC	Main Developer Contractor
N.SIS II	Secțiunea națională în fiecare stat membru
NI-SIS	Interfață națională uniformă
NTP	Protocol de sincronizare în rețea (Network Time Protocol)
SAN	Rețea de stocare (Storage Area Network)
SDH	Ierarhie digitală sincronă (Synchronous Digital Hierarchy)
SIS II	Sistem de informații Schengen din a doua generație (Schengen Information System, second generation)
SMTP	Protocol simplu de transfer de curier (Simple Mail Transport Protocol)
SNMP	Protocol simplu de gestiune de rețea (Simple Network Management Protocol)
s-TESTA	Servicii telematice transeuropene securizate între administratori (Secure Trans-European Services for Telematics between Administrations), o măsură a programului IDABC (Programul pentru furnizarea interoperabilă a serviciilor europene e-guvernare pentru administrațiile publice, întreprinderi și cetățeni. Decizia 2004/387/EC a Parlamentului European și a Consiliului din 21.4.2004).
TCP	Protocol de control al transmisiei (Transmission Control Protocol)
VIS	Sistem de informații privind vizele (Visa Information System)
VPN	Rețea privată virtuală (Virtual Private Network)
WAN	Rețea de arie largă (Wide Area Network)

2. **Privire de ansamblu**

SIS II este format din:

— sistemul central (denumit în continuare „SIS II central"), care cuprinde:

• o funcție de suport tehnic (denumită în continuare „CS-SIS") care conține baza de date a SIS II. Sistemul principal CS-SIS asigură supravegherea tehnică și administrarea, iar un sistem CS-SIS de siguranță poate asigura toate funcțiile sistemului principal CS-SIS, în cazul în care acesta nu funcționează;

• o interfață națională uniformă (denumită în continuare „NI-SIS");

— o secțiune națională (denumită în continuare „N.SIS II") în fiecare dintre statele membre, care cuprinde sistemele naționale de date și care comunică cu SIS II central. O secțiune N.SIS II poate conține un dosar de date (denumit în continuare „copie națională"), care conține o copie completă sau parțială a bazei de date SIS II;

— o infrastructură de comunicații între CS-SIS și NI-SIS (denumită în continuare „infrastructură de comunicații") care furnizează o rețea virtuală criptată consacrată datelor SIS II și schimbului de date dintre birourile SIRENE.

NI-SIS este formată din:

— o interfață națională locală (denumită în continuare „LNI") în fiecare stat membru, care face conexiunea fizică între statul membru și rețeaua de comunicații securizată și conține dispozitivele de criptare consacrate traficului dintre SIS II și SIRENE. LNI este situată pe teritoriul statului membru;

— o interfață națională locală de siguranță, opțională (denumită în continuare „BLNI"), care are exact aceeași structură și funcție ca LNI.

LNI și BLNI trebuie utilizate exclusiv de sistemul SIS II și pentru schimburile SIRENE. Configurația specifică a LNI și BLNI va fi precizată și convenită cu fiecare stat membru pentru a se lua în considerare normele de siguranță, locația fizică și condițiile de instalare, inclusiv prestarea de servicii a furnizorului de rețea, adică conexiunea fizică s-TESTA poate conține mai multe canale VPN pentru alte sisteme, de exemplu, VIS și Eurodac.

— o interfață națională centrală (denumită în continuare „CNI"), care este o aplicație ce securizează accesul la CS-SIS. Fiecare stat membru dispune de propriile puncte logice de acces la CNI via un „firewall" central.

Infrastructura de comunicații dintre CS-SIS și NI-SIS este compusă din:

— rețeaua pentru Servicii telematice transeuropene securizate între administratori (denumită în continuare s-TESTA), care furnizează o rețea virtuală privată și criptată, consacrată datelor SIS II și schimburilor SIRENE.

3. **Acoperire geografică**

Infrastructura de comunicații trebuie să poată acoperi și furniza serviciile cerute tuturor statelor membre:

Toate statele membre UE (Belgia, Franța, Germania, Luxemburg, Țările de Jos, Italia, Portugalia, Spania, Grecia, Austria, Danemarca, Finlanda, Suedia, Cipru, Republica Cehă, Estonia, Ungaria, Letonia, Lituania, Malta, Polonia, Slovacia, Slovenia, Regatul Unit și Irlanda), plus Norvegia, Islanda, Elveția.

În plus, trebuie luată în considerare acoperirea țărilor care tocmai au aderat, România și Bulgaria.

În cele din urmă, infrastructura de comunicații trebuie să poată fi extinsă la orice altă țară sau entitate care are acces la SIS II central (de exemplu, Europol, Eurojust).

4. **Servicii de rețea**

În cazul menționării unui protocol sau a unei arhitecturi, se subînțelege că alte tehnologii, protocoale sau arhitecturi dezvoltate ulterior vor fi acceptate.

4.1. *Structura rețelei*

Arhitectura SIS II utilizează servicii centralizate, care sunt accesibile din diferitele state membre. Din motive de rezistență, aceste servicii centralizate sunt duplicate în două locații diferite, mai exact la Strasbourg, în Franța, și la St Johann im Pongau, în Austria, unde se situează CS-SIS, CU și, respectiv, sistemul de siguranță CS-SIS, BCU.

Unitățile centrale, cea principală și cea de siguranță, trebuie să fie accesibile din diferitele state membre. Țările implicate pot avea mai multe puncte de acces la rețea, o LNI și o BLNI, pentru a face legătura dintre sistemele lor naționale și serviciile centrale.

În afară de conexiunea principală cu serviciile centrale, infrastructura de comunicații poate asigura schimburi de informații suplimentare bilaterale între birourile SIRENE ale diferitelor state membre.

4.2. *Tip de conexiune între CS-SIS principal și CS-SIS de siguranță*

Tipul de conexiune cerut pentru interconexiunea între CS-SIS principal și CS-SIS de siguranță trebuie să fie o buclă SDH sau un echivalent, care să fie accesibilă și pentru tehnologii și arhitecturi ulterioare. Infrastructura SDH va fi utilizată pentru extinderea rețelelor locale ale ambelor unități centrale, pentru a crea un LAN unic omogen. Acest LAN va fi apoi folosit în sincronizarea continuă dintre CU și BCU.

4.3. *Lățimea de bandă*

O condiție esențială a infrastructurii de comunicații este dimensiunea lățimii de bandă pe care aceasta trebuie să fie în măsură să o acorde diferitelor site-uri interconectate și capacitatea sa de a susține această lățime de bandă în cadrul rețelei sale de bază.

Lățimea de bandă necesară pentru LNI și BLNI facultativă va varia pentru fiecare stat membru, în funcție de alegerea acestuia de a folosi copii naționale, căutare centrală sau schimbul de date biometrice.

Dimensiunea reală pe care infrastructura de comunicații va decide să o ofere este fără importanță, din moment ce corespunde cerințelor minime ale fiecărui stat membru.

Fiecare dintre tipurile de site menționate mai sus poate transfera cantități semnificative de date (alfanumerice, biometrice și documente complete) în ambele direcții. Prin urmare, infrastructura de comunicații trebuie să asigure vitezele minime garantate de încărcare și descărcare pentru fiecare conexiune.

Infrastructura de comunicații trebuie să asigure un debit de conexiune variind între 2 Mbps și până la 155 Mbps sau mai mult. Rețeaua trebuie să asigure viteze minime suficiente de încărcare și descărcare pentru fiecare conexiune și trebuie să aibă capacitatea de a susține lățimea de bandă globală a punctelor de acces la rețea.

4.4. *Categorii de servicii*

SIS II central va fi în măsură să trateze, după o ordine a priorităților, cererile/alertele. Ca normă derivată, infrastructura de comunicații va asigura gestiunea traficului în funcție de priorități.

Se presupune că parametrii de rețea care vor permite stabilirea priorităților vor fi fixați de SIS II central pentru toate pachetele care îl cer. Gestiunea documentelor în așteptare va fi asigurată de procedeul „Weighted Fair Queuing". Aceasta implică faptul că infrastructura de comunicații trebuie să poată prelua ordinea de prioritate atribuită pachetelor de date pe sursa LAN și să le trateze în funcție de această ordine în propria rețea de bază. Mai mult, infrastructura de comunicații trebuie să transmită site-ului de la distanță pachetele inițiale care conțin aceeași ordine de prioritate ca aceea fixată în sursa LAN.

4.5. *Protocoale suportate*

SIS II central va folosi mai multe protocoale de comunicare în rețea. Infrastructura de comunicații ar trebui să suporte o categorie largă de protocoale de comunicație în rețea. Protocoalele standard care vor fi suportate sunt HTTP, FTP, NTP, SMTP, SNMP și DNS.

Pe lângă protocoalele standard, infrastructura de comunicații trebuie să poată gestiona diferite protocoale de „tunnelling", protocoale de duplicare SAN și protocoalele proprietare de conexiune Java-to-Java ale BEA WebLogic. Protocoalele de tunnelling, de exemplu IPsec în mod tunel, vor fi utilizate pentru transferul datelor criptate către destinație.

4.6. *Caracteristici tehnice*

4.6.1. Adresare IP

Infrastructura de comunicații trebuie să aibă o serie de adrese IP rezervate care pot fi utilizate numai în cadrul acelei rețele. În cadrul seriei de adrese IP rezervate, SIS II central va utiliza o serie exclusivă de adrese IP care nu vor fi folosite în altă parte.

4.6.2. Suport pentru IPv6

Se presupune că protocolul utilizat de rețelele locale ale statelor membre va fi TCP/IP. Cu toate acestea, unele site-uri vor avea versiunea 4, pe când altele vor avea versiunea 6. Punctele de acces la rețea trebuie să poată juca rolul de portal și trebuie să aibă capacitatea de a opera independent de protocoalele de rețea utilizate de SIS II central sau de N.SIS II.

4.6.3. Routare statică

CU și BCU pot folosi aceeași adresă unică IP pentru comunicațiile către statele membre. Prin urmare, infrastructura de comunicații trebuie să suporte routarea statică.

4.6.4. Debit susținut

Atât timp cât conexiunile CU sau BCU au o rată de descărcare mai mică de 90 %, un stat membru trebuie să poată susține neîntrerupt 100 % din lățimea sa de bandă.

4.6.5. Alte caracteristici

Pentru a susține CS-SIS, infrastructura de comunicații trebuie să respecte un număr minim de caracteristici tehnice.

Timpul de tranzit trebuie să fie (inclusiv la orele de vârf) mai mic sau egal cu 150 ms, în 95 % din pachetele de date, și mai mic de 200 ms, în 100 % din pachete.

Probabilitatea de a pierde pachetele de date trebuie să fie (inclusiv la orele de vârf) mai mică sau egală cu 10^{-4}, în 95 % din pachete, și mai mică de 10^{-3}, în 100 % din pachete.

Caracteristicile mai sus menționate se aplică pentru fiecare punct de acces în parte.

Conexiunea dintre CU și BCU trebuie să aibă un timp de transmisie dus-întors mai mic sau egal cu 60 ms.

4.7. *Rezistență*

CS-SIS a fost concepută pentru a putea îndeplini condiția de disponibilitate ridicată. Din acest motiv, sistemul oferă o rezistență integrată împotriva defecțiunilor propriilor componente, grație duplicării tuturor echipamentelor.

Componentele infrastructurii de comunicații trebuie, de asemenea, să aibă rezistență împotriva defecțiunilor ce pot afecta unul dintre componente. În cazul infrastructurii de comunicații, următoarele componente trebuie să aibă rezistență:

— Rețeaua de bază

— Dispozitivele de routare

— Punctele de prezență

— Conexiunile la bucla locală (inclusiv cablarea fizică redundantă)

— Dispozitivele de siguranță (dispozitive de criptare, „firewall" etc.)

— Toate serviciile generice (DNS, NTP etc.)

— LNI/BLNI.

Mecanismele de siguranță pentru tot echipamentul rețelei trebuie să se declanșeze fără nicio intervenție manuală.

5. **Monitorizare**

Pentru a facilita monitorizarea, instrumentele de monitorizare a infrastructurii de comunicații trebuie să se poată integra în dispozitivele de monitorizare ale organismului responsabil de gestiunea operațională a SIS II central.

6. **Servicii generice**

În afară de rețeaua specializată și de serviciile de siguranță, infrastructura de comunicații trebuie, de asemenea, să ofere și servicii generice.

Trebuie puse în aplicare servicii specializate în cazul ambelor unități centrale, cu scopuri de redundanță.

Infrastructura de comunicații trebuie să ofere următoarele servicii generice opționale:

Serviciu	Informații suplimentare
DNS	În prezent, procedura de siguranță care basculează de la CU la BCU, în cazul defectării sistemului se bazează pe schimbarea adresei IP în cadrul serverului generic DNS.
Releu e-mail	Folosirea unui releu generic e-mail ar putea fi utilă pentru că ar standardiza setările e-mail în diferitele state membre și, spre deosebire de un server specializat, pentru că nu ar consuma resursele de rețea de la CU/BCU. E-mail-urile care utilizează releul generic e-mail trebuie să respecte modelul de siguranță.
NTP	Acest serviciu poate fi utilizat pentru sincronizarea ceasurilor echipamentului de rețea.

7. **Disponibilitate**

CS-SIS, LNI și BLNI trebuie să poată oferi o disponibilitate de 99,99 % pe o perioadă continuă de 28 de zile, independent de disponibilitatea rețelei.

Disponibilitatea infrastructurii de comunicații trebuie să fie de 99,99 %.

8. **Servicii de siguranță**

8.1. *Criptarea rețelei*

SIS II central nu permite transferul în afara LAN fără criptare a datelor cu exigență de înaltă sau foarte înaltă protecție. Trebuie să se verifice ca furnizorul de rețea să nu aibă în niciun caz acces la datele operaționale din SIS II, nici la schimburile SIRENE asociate.

Pentru a menține un înalt nivel de siguranță, infrastructura de comunicații trebuie să permită gestiunea certificatelor/cheilor. Gestiunea și monitorizarea de la distanță a cutiilor de criptare trebuie să fie posibile. Algoritmii de criptare trebuie să îndeplinească cel puțin următoarele condiții:

— Algoritmi de criptare simetrică:

• 3DES (128 biți) sau mai mult.

• Generarea cheii trebuie să depindă de o valoare aleatorie care să nu permită reducerea spațiului de cheie în cazul unui atac.

• Cheile de criptare sau informațiile care pot fi utilizate pentru a genera chei sunt întotdeauna protejate în timpul stocajului.

— Algoritmi de criptare asimetrică:

• RSA (modul 1 024 biți) sau mai mult.

• Generarea cheii trebuie să depindă de o valoare aleatorie care să nu permită reducerea spațiului de cheie în cazul unui atac.

Se va utiliza protocolul de încapsulare a sarcinii utile de siguranță (ESP, RFC2406) în modul tunel. Sarcina utilă și antetul IP de origine vor fi criptate.

Se va utiliza protocolul schimbării cheilor internet (IKE) pentru schimbarea cheilor de sesiune.

Cheile IKE sunt valabile cel mult o zi.

Cheile de sesiune sunt valabile cel mult o oră.

8.2. *Alte dispoziții de siguranță*

Pe lângă protecția punctelor de acces SIS II, infrastructura de comunicații trebuie să protejeze și serviciile generice opționale. Aceste servicii trebuie să fie supuse unor măsuri de protecție comparabile celor din CS-SIS. Prin urmare, toate serviciile generice trebuie să fie protejate cel puțin de un firewall, un antivirus și de un sistem de detectare a intruziunilor. Mai mult, dispozitivele și măsurile de protecție ale serviciilor generice trebuie supuse unei supravegheri de siguranță continue (jurnalizare și urmărire).

Pentru a menține un înalt nivel de siguranță, organizația responsabilă de gestiunea operațională a SIS II central trebuie să fie informată de orice incident de siguranță care survine în infrastructura de comunicații. Prin urmare, infrastructura de comunicații trebuie să permită notificarea rapidă a organizației responsabile de gestiunea operațională a SIS II central asupra incidentelor de siguranță. Toate incidentele de siguranță trebuie semnalate regulat, de exemplu, într-un raport lunar sau ocazional.

9. **Asistență și structură de sprijin**

Furnizorul infrastructurii de comunicații trebuie să pună la dispoziție un serviciu de asistență care să fie în contact cu organizația responsabilă de gestiunea operațională a SIS II central.

10. **Interacțiunea cu alte sisteme**

Infrastructura de comunicații trebuie să împiedice scurgerea de informații dincolo de canalele de comunicație care i-au fost destinate. Pentru aplicarea tehnică, acest fapt implică:

— orice acces neautorizat și/sau necontrolat la alte rețele este strict interzis, inclusiv interconexiunea la internet;

— scurgerea de date către alte sisteme ale rețelei este imposibilă; de exemplu, interconexiunea mai multor VPN IP nu este permisă.

În afară de restricțiile tehnice sus-menționate pe care le impune, infrastructura de comunicații are repercusiuni și asupra serviciului de asistență. Serviciul de asistență nu poate divulga nicio informație privind SIS II central altei entități, în afara celei responsabile de gestiunea operațională a SIS II central.