

**SKLEP KOMISIJE****z dne 16. marca 2007****o določitvi zahtev omrežja za Schengenski informacijski sistem II (3. steber)**

(2007/171/ES)

KOMISIJA EVROPSKIH SKUPNOSTI JE –

Velike Britanije in Severne Irske za sodelovanje pri izvajanju nekaterih določb schengenskega pravnega reda <sup>(3)</sup>.

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti,

ob upoštevanju Sklepa Sveta (ES) št. 2001/886/PNZ z dne 6. decembra 2001 <sup>(1)</sup> o razvoju druge generacije Schengenskega informacijskega sistema (SIS II) in zlasti člena 4(a) Sklepa,

ob upoštevanju naslednjega:

(1) Za razvoj SIS II je treba določiti tehnične specifikacije glede komunikacijskega omrežja, njegovih komponent in posebnih zahtev omrežja.

(2) Komisija in države članice morajo sprejeti ustrezne dogovore zlasti glede elementov enotnega nacionalnega vmesnika v državah članicah.

(3) Ta sklep ne preprečuje sprejetja drugih sklepov Komisije v prihodnosti, povezanih z razvojem SIS II, zlasti glede razvoja varnostnih zahtev.

(4) Tako Uredba Sveta (ES) št. 2424/2001 <sup>(2)</sup> kot Sklep Sveta 2001/886/PNZ urejata razvoj SIS II. Za zagotovitev, da bo obstajal en sam postopek izvajanja za razvoj SIS II kot celote, morajo določbe v tem sklepu odražati določbe Odločbe Komisije, ki določa zahteve omrežja za SIS II, ki jih je treba upoštevati pri uporabi Uredbe (ES) št. 2424/2001.

(5) Združeno kraljestvo sodeluje pri tem sklepu v skladu s členom 5 Protokola o vključitvi schengenskega pravnega reda v okvir Evropske unije, ki je priložen k Pogodbi EU in Pogodbi ES, in členom 8(2) Sklepa Sveta 2000/365/ES z dne 29. maja 2000 o prošnji Združenega kraljestva

(6) Irska sodeluje pri tem sklepu v skladu s členom 5 Protokola o vključitvi schengenskega pravnega reda v okvir Evropske unije, ki je priložen k Pogodbi EU in Pogodbi ES, in člena 5(1) in 6(2) Sklepa Sveta 2002/192/ES z dne 28. februarja 2002 o prošnji Irske za sodelovanje pri izvajanju nekaterih določb schengenskega pravnega reda <sup>(4)</sup>.(7) Kar zadeva Islandijo in Norveško, ta sklep pomeni razvoj določb schengenskega pravnega reda v smislu Sporazuma, sklenjenega med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško o pridružitvi obeh k izvajanju, uporabi in razvoju schengenskega pravnega reda, kar sodi na področje iz točke G člena 1 Sklepa Sveta 1999/437/ES <sup>(5)</sup> o nekaterih izvedbenih predpisih za uporabo tega sporazuma.(8) Kar zadeva Švico, ta sklep pomeni razvoj določb schengenskega pravnega reda v smislu Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda, kar sodi v področje iz točke G člena 1 Sklepa Sveta 1999/437/ES v povezavi s členom 4(1) Sklepa Sveta 2004/849/ES o podpisu in očasni uporabi nekaterih določb navedenega sporazuma v imenu Evropske unije <sup>(6)</sup>.

(9) Ta odločba je akt, ki temelji na schengenskem pravnem redu ali je z njim drugače povezan v smislu člena 3(1) Akta o pristopu.

(10) Ukrepi, predvideni s tem sklepom, so v skladu z mnenjem Odbora, ustanovljenega s členom 5(1) Sklepa (ES) št. 2001/886/PNZ –

<sup>(1)</sup> UL L 328, 13.12.2001, str. 1.<sup>(2)</sup> UL L 328, 13.12.2001, str. 4. Uredba, kakor je bila spremenjena z Uredbo (ES) št. 1988/2006 (UL L 411, 30.12.2006, str. 1).<sup>(3)</sup> UL L 131, 1.6.2000, str. 43. Sklep, kakor je bil spremenjen s Sklepom 2004/926/ES (UL L 395, 31.12.2004, str. 70).<sup>(4)</sup> UL L 64, 7.3.2002, str. 20.<sup>(5)</sup> UL L 176, 10.7.1999, str. 31.<sup>(6)</sup> UL L 368, 15.12.2004, str. 26.

SKLENILA:

*Člen 1*

Tehnične specifikacije, povezane z oblikovanjem fizične arhitekture komunikacijske infrastrukture SIS II, so določene v Prilogi.

V Bruslju, 16. marca 2007

*Za Komisijo*  
Franco FRATTINI  
*Podpredsednik*

---

## PRILOGA

## KAZALO

|       |  |    |
|-------|--|----|
| 1.    | Uvod .....   | 32 |
| 1.1   | Akronimi in okrajšave .....  | 32 |
| 2.    | Splošni pregled .....  | 33 |
| 3.    | Geografska pokritost .....   | 33 |
| 4.    | Omrežne storitve .....   | 34 |
| 4.1   | Struktura omrežja .....  | 34 |
| 4.2   | Vrsta povezave med osnovnim CS-SIS – varnostno kopijo CS-SIS ..... | 34 |
| 4.3   | Pasovna širina .....   | 34 |
| 4.4   | Vrste storitev .....   | 34 |
| 4.5   | Podporni protokoli .....   | 35 |
| 4.6   | Tehnične specifikacije .....                                       | 35 |
| 4.6.1 | Dodeljevanje naslovov IP .....                                     | 35 |
| 4.6.2 | Podpora za IPv6 .....  | 35 |
| 4.6.3 | Dodajanje statičnih smeri .....                                    | 35 |
| 4.6.4 | Vzdrževanje hitrosti pretoka .....                                 | 35 |
| 4.6.5 | Druge specifikacije .....  | 35 |
| 4.7   | Prožnost .....   | 35 |
| 5.    | Spremljanje .....  | 36 |
| 6.    | Splošne storitve .....   | 36 |
| 7.    | Razpoložljivost .....  | 36 |
| 8.    | Varnostne storitve .....   | 36 |
| 8.1   | Šifriranje omrežja .....   | 36 |
| 8.2   | Druge varnostne značilnosti .....                                  | 37 |
| 9.    | Struktura službe za pomoč uporabnikom .....                        | 37 |
| 10.   | Sodelovanje z drugimi sistemi .....                                | 37 |

## 1. Uvod

Ta dokument opisuje obliko komunikacijskega omrežja, komponente, ki jih vsebuje, in posebne zahteve omrežja.

### 1.1 Akronimi in okrajšave

Ta razdelek opisuje akronime, ki se uporabljajo v dokumentu.

| Akronimi in okrajšave | Obrazložitev   |
|-----------------------|--|
| BLNI                  | Lokalni nacionalni vmesnik za varnostno kopiranje (Backup Local National Interface)  |
| CEP                   | Centralna končna točka (Central End Point)   |
| CNI                   | Centralni nacionalni vmesnik (Central National Interface)  |
| CS                    | Centralni sistem   |
| CS-SIS                | Tehnični podporni del, ki vsebuje zbirko podatkov SIS II   |
| DNS                   | Strežnik za domenska imena (Domain Name Server)  |
| FCIP                  | Optični kanal preko IP (Fibre Channel over IP)   |
| FTP                   | Protokol, ki temelji na sistemu odjemalec-strežnik (File Transport Protocol)   |
| HTTP                  | Protokol za izmenjavo nadbisedila (Hyper Text Transfer Protocol)   |
| IP                    | Internetni protokol  |
| LAN                   | Lokalno omrežje (Local Area Network)   |
| LNI                   | Lokalni nacionalni vmesnik (Local National Interface)  |
| Mb/s                  | Megabitov na sekundo   |
| MDC                   | Glavni razvijalec, izvajalec (Main Developer Contractor)   |
| N.SIS II              | Nacionalni del v vsaki državi članici  |
| NI-SIS                | Enoten nacionalni vmesnik  |
| NTP                   | Omrežni časovni protokol (Network Time Protocol)   |
| SAN                   | Omrežje pomnilniških naprav (Storage Area Network)   |
| SDH                   | Sinhrona digitalna hierarhija (Synchronous Digital Hierarchy)  |
| SIS II                | Schengenski informacijski sistem, druga generacija   |
| SMTP                  | Preprost protokol za prenos elektronske pošte (Simple Mail Transport Protocol)   |
| SNMP                  | Preprost protokol za upravljanje omrežja (Simple Network Management Protocol)  |
| s-TESTA               | Varne vseevropske telematske storitve med upravami; je ukrep programa IDABC (interoperabilno zagotavljanje vseevropskih e-vladnih storitev javnim upravam, podjetjem in državljanom; Sklep Evropskega parlamenta in Sveta št. 2004/387/ES z dne 21. aprila 2004) |
| TCP                   | Protokol za krmiljenje prenosa (Transmission Control Protocol)   |
| VIS                   | Vizumski informacijski sistem  |
| VPN                   | Navidezno zasebno omrežje (Virtual Private Network)  |
| WAN                   | Prostrano omrežje (Wide Area Network)  |

## 2. Splošni pregled

SIS II sestavljajo:

- centralni sistem (v nadaljnjem besedilu „Centralni SIS II“), ki ga sestavljata:
  - tehnični podporni del (v nadaljnjem besedilu „CS-SIS“), ki vsebuje zbirko podatkov SIS II. Osnovni CS-SIS izvaja tehnični nadzor in upravljanje, varnostna kopija CS-SIS pa zagotavlja opravljanje vseh funkcij osnovnega CS-SIS v primeru okvare tega sistema,
  - enoten nacionalni vmesnik (v nadaljnjem besedilu „NI-SIS“),
- nacionalni del (v nadaljnjem besedilu „N.SIS II“) v vsaki državi članici, sestavljen iz nacionalnih podatkovnih sistemov, ki so povezani s Centralnim SIS II. N.SIS II lahko vsebuje podatkovno zbirko (v nadaljnjem besedilu „nacionalna kopija“), ki vsebuje celotno ali delno kopijo zbirke podatkov SIS II,
- komunikacijska infrastruktura med CS-SIS in NI-SIS (v nadaljnjem besedilu „komunikacijska infrastruktura“), ki zagotavlja šifrirano navidezno omrežje, namenjeno podatkom SIS II in izmenjavi podatkov med uradi SIRENE.

NI-SIS sestavljajo:

- en lokalni nacionalni vmesnik (v nadaljnjem besedilu „LNI“) v vsaki državi članici, ki fizično povezuje državo članico z varnim komunikacijskim omrežjem in vsebuje naprave za šifriranje, namenjene prometu podatkov SIS II in SIRENE. LNI se nahaja v državi članici,
- neobvezen lokalni nacionalni vmesnik za varnostno kopiranje (v nadaljnjem besedilu „BLNI“), ki ima popolnoma enako vsebino in funkcijo kot LNI.

LNI in BLNI se uporabljata samo za sistem SIS II in za izmenjavo podatkov SIRENE. Posebna konfiguracija LNI in BLNI bo podrobno določena in dogovorjena z vsako posamezno državo članico, da bodo upoštewane varnostne zahteve, fizična lokacija in pogoji namestitve, vključno z zagotavljanjem storitev ponudnika omrežja, kar pomeni, da lahko fizična povezava s-TESTA vsebuje več tunelov VPN za druge sisteme, na primer VIS in Eurodac,

- centralni nacionalni vmesnik (v nadaljnjem besedilu „CNI“), ki je aplikacija za varni dostop do CS-SIS. Vsaka država članica ima ločene logične dostopne točke do CNI preko centralnega požarnega zidu.

Komunikacijsko infrastrukturo med CS-SIS in NI-SIS sestavlja:

- omrežje za varne vseevropske telematske storitve med upravami (v nadaljnjem besedilu s-TESTA), ki zagotavlja šifrirano, navidezno, zasebno omrežje, namenjeno prometu podatkov SIS II in SIRENE.

## 3. Geografska pokritost

Komunikacijska infrastruktura mora zajemati in zagotavljati potrebne storitve vsem državam članicam:

vse države članice EU (Belgija, Francija, Nemčija, Luksemburg, Nizozemska, Italija, Portugalska, Španija, Grčija, Avstrija, Danska, Finska, Švedska, Ciper, Češka, Estonija, Madžarska, Latvija, Litva, Malta, Poljska, Slovaška, Slovenija, Združeno kraljestvo, Irska) in Norveška, Islandija, Švica.

Poleg tega je treba zagotoviti tudi pokritost držav pristopnic Romunije in Bolgarije.

Končno mora komunikacijska infrastruktura zagotavljati možnost, da se lahko razširi na katero koli drugo državo ali subjekt, ki pristopi k Centralnemu SIS II (npr. Europol, Eurojust).

#### 4. Omrežne storitve

V primerih, ko je omenjen protokol ali arhitektura, je treba razumeti, da so sprejemljive tudi enakovredne prihodnje tehnologije, protokoli in arhitektura.

##### 4.1 Struktura omrežja

Arhitektura SIS II uporablja centralizirane storitve, ki so dostopne iz različnih držav članic. Za namene prožnosti so te centralizirane storitve podvojene na dveh različnih lokacijah, in sicer Strasbourg v Franciji in St Johann im Pongau v Avstriji. Te storitve vključujejo CS-SIS, CU in varnostne kopije CS-SIS, BCU.

Centralne enote, glavne in varnostne kopije, morajo biti dostopne iz različnih držav članic. Sodelujoče države imajo lahko več dostopnih točk do omrežja, LNI in BLNI, da povežejo svoje nacionalne sisteme s centralnimi storitvami.

Poleg glavne povezljivosti s centralnimi storitvami mora komunikacijska infrastruktura podpirati tudi dvostransko dodatno izmenjavo podatkov med uradi SIRENE v različnih državah članicah.

##### 4.2 Vrsta povezave med osnovnim CS-SIS – varnostno kopijo CS-SIS

Zahtevana vrsta povezave za medsebojno povezljivost med osnovnim CS-SIS in varnostno kopijo CS-SIS mora biti obroč SDH ali ekvivalent, kar pomeni, da mora biti odprta tudi za nove prihodnje arhitekture in tehnologije. Infrastruktura SDH se bo uporabljala za razširitev lokalnih omrežij obeh centralnih enot, da se ustvari en sam brezšiven LAN (seamless LAN). Ta LAN se bo nato uporabljal za nepretrgano sinhronizacijo med CU in BCU.

##### 4.3 Pasovna širina

Ključna zahteva za komunikacijsko infrastrukturo je pasovna širina, ki jo lahko zagotovi različnim medsebojno povezanim stranem in sposobnost infrastrukture, da podpira to pasovno širino znotraj svojega hrbtničnega omrežja.

Pasovna širina, ki je potrebna za LNI in neobvezen BLNI, bo različna za vsako državo članico, odvisna pa bo predvsem od izbire uporabe nacionalnih kopij, centralnega iskanja in izmenjave biometričnih podatkov.

Dejanske velikosti, ki jih komunikacijska infrastruktura namerava nuditi, so nepomembne, če izpolnjujejo minimalno potrebo posamezne države članice.

Vsaka od zgoraj navedenih vrst strani lahko prenese veliko količino podatkov (alfanumeričnih, biometričnih in celotnih dokumentov) v obe smeri. Zato mora komunikacijska infrastruktura zagotoviti zadostno minimalno hitrost nalaganja in prenašanja podatkov za vsako povezavo.

Komunikacijska infrastruktura mora nuditi obseg povezave od 2 Mb/s do 155 Mb/s ali več. Omrežje mora zagotoviti zadostno minimalno hitrost nalaganja in prenašanja podatkov za vsako povezavo in njegov obseg mora biti zadosten, da podpira celotno pasovno širino dostopnih točk do omrežja.

##### 4.4 Vrste storitev

Centralni SIS II bo podprl zmogljivost prednostnega razvrščanja iskanj/razpisov ukrepov. Iz tega izhaja zahteva, da bo komunikacijska infrastruktura podprla tudi možnost prednostnega razvrščanja prometa podatkov.

Za parametre omrežnega prednostnega razvrščanja se šteje, da bodo določeni s strani Centralnega SIS II za vse pakete, ki bodo to zahtevali. Uporabil se bo mehanizem „Weighted Fair Queuing“. To pomeni, da mora biti komunikacijska infrastruktura sposobna prevzeti prednostno razvrščanje, določeno za pakete na izvirmem LAN, in ustrezno obravnavati pakete v okviru svojega hrbtničnega omrežja. Poleg tega mora komunikacijska infrastruktura preko oddaljene strani posredovati začetne pakete, ki vsebujejo enako prednostno razvrščanje, kot je določeno v izvirmem LAN.

#### 4.5 Podporni protokoli

Centralni SIS II bo uporabljal več različnih omrežnih komunikacijskih protokolov. Komunikacijska infrastruktura mora podpirati vrsto omrežnih komunikacijskih protokolov. Standardni protokoli, ki bodo podprti, so HTTP, FTP, NTP, SMTP, SNMP in DNS.

Poleg standardnih protokolov mora biti komunikacijska infrastruktura prilagojena za upravljanje različnih tunelskih protokolov, protokolov za podvojevanje SAN in lastniških protokolov tipa Java-to-Java tehnologije BEA WebLogic. Tunelski protokoli, npr. IPsec v tunelskem načinu, se bodo uporabljali za prenos šifriranega prometa podatkov na njegov cilj.

#### 4.6 Tehnične specifikacije

##### 4.6.1 Dodeljevanje naslovov IP

Komunikacijska infrastruktura mora imeti na voljo več rezerviranih IP-naslovov, ki se lahko uporabljajo samo znotraj tega omrežja. V okviru rezerviranega IP razpona bo Centralni SIS II uporabljal določene IP-naslove, ki se drugje ne bodo uporabljali.

##### 4.6.2 Podpora za IPv6

Mogoče je domnevati, da bo protokol, ki se bo uporabljal za lokalna omrežja držav članic, protokol TCP/IP. Vendar bodo nekatere strani temeljile na verziji 4, druge pa na verziji 6. Dostopne točke do omrežja morajo nuditi možnost, da delujejo kot prehod, in delovati morajo neodvisno od omrežnih protokolov, uporabljenih v Centralnem SIS II kot tudi v N.SIS II.

##### 4.6.3 Dodajanje statičnih smeri

CU in BCU lahko uporabljata isti IP-naslov za komuniciranje z državami članicami. Zato mora komunikacijska infrastruktura podpirati dodajanje statičnih smeri.

##### 4.6.4 Vzdrževanje hitrosti pretoka

Dokler ima CU ali BCU povezava hitrost nalaganja nižjo od 90 %, mora biti dana država članica sposobna trajno vzdrževati 100 % pasovne širine, določene za to povezavo.

##### 4.6.5 Druge specifikacije

Za podporo CS-SIS mora komunikacijska infrastruktura izpolnjevati vsaj minimalne tehnične specifikacije:

Zamuda pri prenosu mora biti (vključno z najbolj zasedenimi urami) 150 ms ali manj v 95 % paketov in manj kot 200 ms v 100 % paketov.

Njena verjetnost izgube paketa mora biti (vključno z najbolj zasedenimi urami)  $10^{-4}$  ali manj v 95 % paketov in manj kot  $10^{-3}$  v 100 % paketov.

Zgoraj navedene specifikacije je treba upoštevati za vsako dostopno točko posebej.

Povezava med CU in BCU mora imeti povratno zamudo 60 ms ali manj.

#### 4.7 Prožnost

CS-SIS je bil oblikovan z zahtevo visoke razpoložljivosti. Zato ima sistem vgrajeno prožnost s podvajanjem vse opreme za primere motenj delovanja komponent.

Komponente komunikacijske infrastrukture morajo biti prožne tudi v primeru okvare. V zvezi s komunikacijsko infrastrukturo to pomeni, da morajo biti prožne naslednje komponente:

— Hrbtениčno omrežje

— Usmerjevalne naprave

- Točke prisotnosti
- Povezave lokalne zanke (vključno z odvečnimi kabelskimi povezavami)
- Varnostne naprave (kripto naprave, požarni zidovi itd.)
- Vse splošne storitve (DNS, NTP itd.)
- LNI/BLNI.

Mehanizmi za nadomestni način delovanja za vso opremo omrežja morajo delovati brez ročnega posredovanja.

## 5. Spremljanje

Za olajšanje spremljanja morajo biti orodja za spremljanje komunikacijske infrastrukture takšna, da se lahko vključijo v naprave za nadzor organizacij, odgovornih za operativno upravljanje Centralnega SIS II.

## 6. Splošne storitve

Poleg namenskega omrežja in varnostnih storitev mora komunikacijska infrastruktura nuditi tudi splošne storitve.

Namenske storitve je treba izvajati znotraj obeh centralnih enot za namene redundance.

V komunikacijski infrastrukturi morajo biti na voljo naslednje izbirne splošne storitve:

| Storitev             | Dodatne informacije   |
|----------------------|---|
| DNS                  | Sedanji postopek za nadomestni način delovanja za preklapljanje iz CU na BCU v primeru izpada omrežja temelji na spremembi IP-naslova znotraj splošnega strežnika DNS.  |
| Posredovanje e-pošte | Uporaba splošnega posredovanja e-pošte bi lahko bila koristna za standardizacijo nastavitve e-naslova za različne države članice, ki v nasprotju z namenskim strežnikom ne izrablja omrežnih virov iz CU/BCU.<br>E-pošta, ki uporablja splošno posredovanje e-pošte, mora kljub temu upoštevati varnostno predlogo. |
| NTP                  | Ta storitev se lahko uporablja za sinhronizacijo ur v opremi omrežja.   |

## 7. Razpoložljivost

CS-SIS ter LNI in BLNI morajo omogočiti 99,99 % razpoložljivost v obdobju 28 dni neprekinjenega delovanja brez razpoložljivosti omrežja.

Razpoložljivost komunikacijske infrastrukture mora biti 99,99 %.

## 8. Varnostne storitve

### 8.1 Šifriranje omrežja

Centralni SIS II ne dovoljuje prenosa podatkov z visokimi ali zelo visokimi varnostnimi zahtevami izven LAN brez šifriranja. Zagotoviti je treba, da ponudnik omrežja na noben način ne bo imel dostopa do operativnih podatkov SIS II kot tudi do podobne izmenjave podatkov SIRENE.

Da bi ohranila visoko stopnjo varnosti, mora komunikacijska infrastruktura omogočiti upravljanje certifikatov/ključev. Omogočeno mora biti skrbništvo na daljavo in spremljanje naprav za šifriranje na daljavo. Algoritmi šifriranja morajo izpolnjevati najmanj naslednje zahteve:



— Simetrični algoritmi šifriranja:

- 3DES (128 bitov) ali boljši,
- generiranje ključev mora biti odvisno od naključne vrednosti, ki ne dopušča zmanjšanja prostora za ključ, če je napadena,
- ključi za šifriranje ali informacije, ki se lahko uporabljajo za izpeljevanje ključev so vedno zaščiteni, če so na pomnilniškem ključu 002E.

— Asimetrični algoritmi šifriranja:

- RSA (1 024 bit modul) ali boljši,
- generiranje ključev mora biti odvisno od naključne vrednosti, ki ne dopušča zmanjšanja prostora za ključ, če je napadena.

Uporabi se protokola za zavarovanje vsebine s šifriranjem (ESP, RFC2406). Uporabljen bo v tunelskem načinu. Vsebina in originalna IP-glava bosta šifrirana.

Za izmenjavo sejnih ključev se uporabi protokol upravljanja z varnostnimi ključi (IKE).

Ključni IKE ne bodo veljavni več kot 1 dan.

Sejni ključni ne bodo veljavni več kot 1 uro.

#### 8.2 Druge varnostne značilnosti

Poleg zaščite dostopnih točk do SIS II mora komunikacijska infrastruktura zaščititi tudi izbirne splošne storitve. Te storitve morajo izpolnjevati iste zaščitne ukrepe, primerljive s tistimi v CS-SIS. Vse splošne storitve morajo biti zato zaščitene najmanj s požarnim zidom, protivirusno zaščito in s sistemom za zaznavanje vsiljivcev. Poleg tega morajo biti naprave za splošne storitve in njihovi zaščitni ukrepi pod stalnim varnostnim nadzorom (beleženje in spremljanje).

Za zagotovitev visoke stopnje varnosti se mora organizacija, odgovorna za operativno upravljanje centralnega SIS II, zavedati vseh incidentov v zvezi z varnostjo, do katerih lahko pride v komunikacijski infrastrukturi. Zato mora komunikacijska infrastruktura omogočati, da se incidenti v zvezi z varnostjo brez zamude sporočijo organizacijam, odgovornim za operativno upravljanje centralnega SIS II. Vsi incidenti v zvezi z varnostjo morajo biti redno zabeleženi, npr. mesečna poročila in *ad hoc* poročila.

#### 9. Struktura službe za pomoč uporabnikom

Ponudnik komunikacijske infrastrukture mora zagotoviti službo za pomoč uporabnikom, ki sodeluje z organizacijo, odgovorno za operativno upravljanje za centralni SIS II.

#### 10. Sodelovanje z drugimi sistemi

Komunikacijska infrastruktura mora zagotoviti, da podatki ne gredo izven določenih komunikacijskih kanalov. Za tehnično izvajanje to pomeni, da:

- je vsak nedovoljen in/ali nenadzorovan dostop do drugih omrežij strogo prepovedan. To vključuje medsebojno povezljivost z internetom,
- ne sme priti do prehajanja podatkov v druge sisteme v omrežju; npr. medsebojna povezljivost z različnimi IP navideznih zasebnih omrežij (VPN) ni dovoljena.

Poleg zgoraj omenjenih tehničnih omejitev, ki jih povzročajo, vpliva tudi na službo za pomoč uporabnikom informacijske infrastrukture. Služba za pomoč uporabnikom ne sme nikomur posredovati nobenih podatkov glede centralnega SIS II, razen organizaciji, odgovorni za operativno upravljanje za centralni SIS II.