KOMISIJOS SPRENDIMAS

2007 m. kovo 16 d.

nustatantis Šengeno informacinės sistemos II tinklo reikalavimus (trečiasis ramstis)

(2007/171/EB)

EUROPOS BENDRIJŲ KOMISIJA,

atsižvelgdama į Europos Sąjungos sutartį,

atsižvelgdama į 2001 m. gruodžio 6 d. Tarybos sprendimą 2001/886/TVR dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo [1], ypač į jo 4 straipsnio a dalį,

kadangi:

(1) Siekiant sukurti SIS II būtina nustatyti ryšių tinklo ir jo sudedamųjų dalių technines specifikacijas bei konkrečius tinklo reikalavimus.

(2) Komisija ir valstybės narės turėtų priimti atitinkamus tarpusavio susitarimus, visų pirma dėl valstybėse narėse esančios vienodos nacionalinės sąsajos elementų.

(3) Šis sprendimas nepažeidžia galimybės ateityje priimti kitus Komisijos sprendimus, susijusius su SIS II kūrimu, pirmiausiai dėl saugumo reikalavimų nustatymo.

(4) SIS II kūrimas reglamentuojamas Tarybos reglamentu (EB) Nr. 2424/2001 [2] ir Tarybos sprendimu 2001/886/TVR. Siekiant užtikrinti, kad būtų vykdomas vienas įgyvendinimo procesas visai SIS II kurti, šio sprendimo nuostatos turėtų atitikti Komisijos sprendimo, nustatančio SIS II tinklo reikalavimus, nuostatas, kurios turi būti priimtos taikant Reglamentą (EB) Nr. 2424/2001.

(5) Jungtinė Karalystė taiko šį sprendimą pagal Protokolo dėl Šengeno *acquis* integravimo į Europos Sąjungos sistemą, pridėto prie ES sutarties ir EB sutarties, 5 straipsnį ir 2000 m. gegužės 29 d. Tarybos sprendimo 2000/365/EB dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės prašymo dalyvauti taikant kai kurias Šengeno *acquis* nuostatas [3] 8 straipsnio 2 dalį.

(6) Airija taiko šį sprendimą pagal Protokolo dėl Šengeno *acquis* integravimo į Europos Sąjungos sistemą, pridėto prie ES sutarties ir EB sutarties, 5 straipsnį ir 2002 m. vasario 28 d. Tarybos sprendimo 2002/192/EB dėl Airijos prašymo dalyvauti įgyvendinant kai kurias Šengeno *acquis* nuostatas [4] 5 straipsnio 1 dalį ir 6 straipsnio 2 dalį.

(7) Kalbant apie Islandiją ir Norvegiją, šiuo sprendimu plėtojamos Šengeno *acquis* nuostatos, kaip apibrėžta Europos Sąjungos Tarybos, Islandijos Respublikos ir Norvegijos Karalystės sudarytame susitarime dėl šių dviejų valstybių asociacijos įgyvendinant, taikant ir plėtojant Šengeno *acquis* Tarybos sprendimo 1999/437/EB [5] dėl tam tikrų priemonių taikant šį susitarimą 1 straipsnio G punkte nurodytoje srityje.

(8) Kalbant apie Šveicariją, šiuo sprendimu plėtojamos Šengeno *acquis* nuostatos, kaip apibrėžta Europos Sąjungos, Europos bendrijos ir Šveicarijos Konfederacijos pasirašytame susitarime dėl Šveicarijos Konfederacijos asociacijos įgyvendinant, taikant ir plėtojant Šengeno *acquis*, Tarybos sprendimo 1999/437/EB 1 straipsnio G punkte, kuris siejamas su Tarybos sprendimo 2004/849/EB [6] dėl šio susitarimo pasirašymo Europos Sąjungos vardu ir dėl laikino tam tikrų nuostatų taikymo 4 straipsnio 1 dalimi, nurodytoje srityje.

(9) Šis sprendimas yra Šengeno *acquis* pagrindu priimtas arba kitaip su juo susijęs aktas, kaip apibrėžta Stojimo akto 3 straipsnio 1 dalyje.

(10) Šiame sprendime numatytos priemonės atitinka Sprendimo 2001/886/TVR 5 straipsnio 1 dalimi įsteigto komiteto nuomonę,

---

[1] OL L 328, 2001 12 13, p. 1.

[2] OL L 328, 2001 12 13, p. 4. Reglamentas su pakeitimais, padarytais Reglamentu (EB) Nr. 1988/2006 (OL L 411, 2006 12 30, p. 1).

[3] OL L 131, 2000 6 1, p. 43. Sprendimas su pakeitimais, padarytais Sprendimu 2004/926/EB (OL L 395, 2004 12 31, p. 70).

[4] OL L 64, 2002 3 7, p. 20.

[5] OL L 176, 1999 7 10, p. 31.

[6] OL L 368, 2004 12 15, p. 26.

NUSPRENDĖ:

1 straipsnis

Priede pateikiamos SIS II ryšių infrastruktūros fizinės architektūros projekto techninės specifikacijos.

Priimta Briuselyje, 2007 m. kovo 16 d.

Komisijos vardu
Franco FRATTINI
Pirmininko pavaduotojas

PRIEDAS

TURINYS

1. **Įvadas**

Šiame dokumente aprašomas ryšių tinklo projektas, šio tinklo sudedamosios dalys ir specialūs tinklo reikalavimai.

1.1. *Akronimai ir santrumpos*

Šioje dalyje pateikiami dokumente vartojami akronimai.

Akronimai ir santrumpos	Paaiškinimas
BLNI	Atsarginė vietinė nacionalinė sąsaja
CEP	Pagrindinis galinis taškas
CNI	Centrinė nacionalinė sąsaja
CS	Centrinė sistema
CS-SIS	Techninio palaikymo funkcija, kurią sudaro SIS II duomenų bazė
DNS	Domenų vardų serveris
FCIP	Optinė jungtis naudojant IP
FTP	Bylų perdavimo protokolas
HTTP	Hiperteksto perdavimo protokolas
IP	Interneto protokolas
LAN	Vietinis tinklas
LNI	Vietinė nacionalinė sąsaja
Mb/s	Megabitų per sekundę
MDC	Pagrindinis sistemos kūrimo rangovas
N.SIS II	Nacionalinė sekcija kiekvienoje valstybėje narėje
NI-SIS	Vienoda nacionalinė sąsaja
NTP	Tinklo įrenginių laikrodžių sinchronizavimo protokolas
SAN	Vietinis laikmenų tinklas
SDH	Sinchroninė skaitmeninė hierarchija
SIS II	Antros kartos Šengeno informacinė sistema
SMTP	Paprastasis pašto persiuntimo protokolas
SNMP	Paprastasis tinklo valdymo protokolas
s-TESTA	Saugios europinės telematinių tinklų paslaugos valstybės valdymo institucijoms – tai IDABC programos priemonė (suderintas paneuropinių e. valdžios paslaugų teikimas valstybės valdymo institucijoms, verslo subjektams ir piliečiams. 2004 m. balandžio 21 d. Europos Parlamento ir Tarybos sprendimas 2004/387/EB).
TCP	Perdavimo valdymo protokolas
VIS	Vizų informacinė sistema
VPN	Virtualusis privatus tinklas
WAN	Platusis tinklas

2. **Bendroji apžvalga**

SIS II sudaro:

— centrinė sistema (toliau – centrinė SIS II), kuri sudaryta iš:

• techninio palaikymo funkcijos (toliau – CS-SIS), kurią sudaro SIS II duomenų bazė. Pagrindinė CS-SIS atlieka techninės priežiūros ir administravimo funkcijas, o atsarginė CS-SIS gali užtikrinti visas pagrindinės CS-SIS funkcijas šios sistemos gedimo atveju,

• vienodos nacionalinės sąsajos (toliau – NI-SIS),

— nacionalinė sekcija (toliau – N.SIS II) kiekvienoje valstybėje narėje, kurią sudaro nacionalinės duomenų sistemos, palaikančios ryšį su centrine SIS II. NS-SIS gali būti duomenų byla (toliau – nacionalinė kopija), kurią sudaro visa ar dalinė SIS II duomenų bazės kopija,

— CS-SIS ir NI-SIS ryšių infrastruktūra (toliau – ryšių infrastruktūra), kuri užtikrina šifruotą virtualų tinklą, skirtą SIS II duomenims perduoti ir keistis duomenimis tarp SIRENE biurų.

NI-SIS, kurią sudaro:

— po vieną vietinę nacionalinę sąsają (toliau – LNI) kiekvienoje valstybėje narėje – tokia sąsaja fiziškai prijungia valstybę narę prie saugaus ryšių tinklo; šią sąsają sudaro šifravimo įranga, skirta SIS II ir SIRENE duomenų srautams. LNI yra valstybių narių teritorijoje,

— neprivaloma atsarginė vietinė nacionalinė sąsaja (toliau – BLNI), kurios turinys ir funkcijos yra visiškai tokie patys kaip LNI.

LNI ir BLNI naudojamos tik SIS II sistemai ir SIRENE duomenų apsikeitimams. Siekiant atsižvelgti į saugumo reikalavimus, fizinę buvimo vietą ir įrengimo sąlygas, taip pat tinklo paslaugų teikėjo teikiamas paslaugas (t. y. fizinė s-TESTA jungtis gali turėti keletą VPN kanalų, skirtų kitoms sistemoms, pavyzdžiui, VIS ir *Eurodac*), konkreti LNI ir BLNI konfigūracija bus nustatyta kiekvienai valstybei narei atskirai su jomis dėl to susitarus;

— centrinė nacionalinė sąsaja (toliau – CNI) – tai programa, užtikrinanti prieigą prie CS-SIS. Kiekviena valstybė narė turi atskirus loginius sąsajos taškus, skirtus prisijungti prie CNI per centrinę užkardą.

CS-SIS ir NI-SIS ryšių infrastruktūrą sudaro:

— saugios europinės telematinių tinklų paslaugos valstybės valdymo institucijoms (toliau – s-TESTA), kurios užtikrina šifruoto, virtualaus ir privataus tinklo, skirto perduoti SIS II duomenis ir SIRENE duomenų srautus, paslaugas.

3. **Geografinė aprėptis**

Ryšių infrastruktūra turi aprėpti visas valstybes nares ir joms užtikrinti būtinas paslaugas.

Visos ES valstybės narės (Belgija, Prancūzija, Vokietija, Liuksemburgas, Nyderlandai, Italija, Portugalija, Ispanija, Graikija, Austrija, Danija, Suomija, Švedija, Kipras, Čekija, Estija, Vengrija, Latvija, Lietuva, Malta, Lenkija, Slovakija, Slovėnija, Jungtinė Karalystė ir Airija) bei Norvegija, Islandija ir Šveicarija.

Be to, naujai įstojusios šalys – Rumunija ir Bulgarija – taip pat turi patekti į aprėpiamą teritoriją.

Galiausiai ryšių infrastruktūros pajėgumai turi būti tokie, kad paslaugas būtų galima teikti bet kuriai šaliai ar institucijai, prisijungusiai prie centrinės SIS II (pvz., Europolui, Eurojustui).

4. **Tinklo paslaugos**

Kai minimas koks nors protokolas ar architektūra, reikėtų suprasti, kad susijusios ateities technologijos, protokolai ar architektūra taip pat galės būti naudojami.

4.1. *Tinklo struktūra*

SIS II architektūrai teikiamos centralizuotos paslaugos, kuriomis galima naudotis iš skirtingų valstybių narių. Siekiant stabilaus sistemos veikimo, šių centralizuotų paslaugų centrai įsteigti dviejose vietovėse – Strasbūre (Prancūzija) yra CS-SIS (CU), o St Johann im Pongau (Austrija) yra atsarginė CS-SIS (BCU).

Turi būti užtikrinta galimybė prisijungti prie sistemos centrų – pagrindinio ir atsarginio – iš skirtingų valstybių narių. Dalyvaujančios šalys gali turėti keletą tinklo prieigos taškų, LNI ir BLNI, skirtų sąveikai tarp nacionalinės sistemos ir centralizuotų paslaugų.

Be pagrindinės prisijungimo prie centralizuotų paslaugų funkcijos, ryšių infrastruktūra turi užtikrinti ir papildomą abipusių informacijos mainų tarp valstybių narių SIRENE biurų funkciją.

4.2. *Pagrindinės CS-SIS ir atsarginės CS-SIS sujungimo būdas*

Sąveikai tarp pagrindinės CS-SIS ir atsarginės CS-SIS užtikrinti turi būti naudojamas sinchroninės skaitmeninės hierarchijos (SDH) žiedas ar atitinkama priemonė, t. y. tokios priemonės, kurios leistų ateityje naudoti naują architektūrą ir naujas technologijas. SDH infrastruktūra bus naudojama abiejų sistemos centrų vietiniams tinklams išplėsti siekiant sukurti vieną vientisą vietinį tinklą (LAN). Toks LAN vėliau būtų naudojamas nuolatinei CU ir BCU sinchronizacijai.

4.3. *Dažnių juostos plotis*

Svarbiausias ryšių infrastruktūrai taikomas reikalavimas – dažnių juostos plotis, kurį ji gali užtikrinti skirtingoms tarpusavyje sujungtoms sistemoms; toks pat dažnių juostos plotis turi būti užtikrinamas ir pagrindiniame tinkle.

Kiekvienos valstybės narės LNI ir neprivalomai BLNI skirtos dažnių juostos plotis skirsis atsižvelgiant į tai, ar bus naudojamos nacionalinės kopijos, paieškos centrinėje sistemoje ir keitimosi biometriniais duomenimis funkcijos.

Realus dažnių juostos plotis, kurį užtikrina ryšių infrastruktūra, nėra svarbus, jeigu jis tenkina minimalius kiekvienos valstybės narės poreikius.

Kiekviena iš pirmiau minėtų sistemų gali į abi puses siųsti didelius duomenų kiekius (radinius skaitmeninius bei biometrinius duomenis ir visus dokumentus). Todėl ryšių infrastruktūra turi užtikrinti mažiausią pakankamą duomenų išsiuntimo ir atsiuntimo greitį kiekvieno prisijungimo metu.

Ryšių infrastruktūra turi užtikrinti, kad ryšio greitis būtų nuo 2 Mb/s iki 155 Mb/s arba didesnis. Tinklo pajėgumas turi būti toks, kad būtų užtikrintas mažiausias pakankamas duomenų išsiuntimo ir atsiuntimo greitis kiekvieno prisijungimo metu ir kad būtų galima aptarnauti bendrą visų tinklo prieigos taškų dažnių juostos plotį.

4.4. *Paslaugų kategorijos*

Centrinė SIS II užtikrins užklausų ir (arba) įspėjimų pirmenybės nustatymo funkciją. Ryšių infrastruktūrai bus taikomas papildomas reikalavimas užtikrinti duomenų srautų pirmenybės nustatymą.

Laikoma, kad pirmenybės nustatymo tinkle parametrus visiems duomenų paketams, kuriems taikomas toks reikalavimas, nustato centrinė SIS II. Bus taikomas pagrįsto teisingo eiliškumo (angl. *Weighted Fair Queuing*) principas. Tai reiškia, kad ryšių infrastruktūra turi būti pajėgi perimti tokią pirmenybės tvarką, kokia duomenų paketams nustatoma šaltinio LAN, ir savo pagrindiniame tinkle tuos duomenų paketus apdoroti atitinkama tvarka. Be to, ryšių infrastruktūra turi užtikrinti, kad pirminiai duomenų paketai į nuotolines sistemas būtų perduodami tokia pat tvarka, kokia buvo nustatyta šaltinio LAN.

4.5. *Naudotini protokolai*

Centrinėje SIS II bus naudojami keli tinklo ryšio protokolai. Ryšių infrastruktūroje turėtų būti naudojami įvairūs tinklo ryšio protokolai. Standartiniai naudotini protokolai – HTTP, FTP, NTP, SMTP, SNMP ir DNS.

Be standartinių protokolų ryšių infrastruktūra turi palaikyti įvairius tuneliavimo protokolus, SAN dubliavimo protokolus ir patentuotus *BEA WebLogic* serverio *Java-to-Java* ryšio protokolus. Šifruotų duomenų srautui perduoti į paskirties vietą bus naudojami tuneliavimo protokolai, pvz., IPsec tuneliavimo režimu.

4.6. *Techninės specifikacijos*

4.6.1. IP adresacija

Ryšių infrastruktūroje turi būti rezervuota keletas IP adresų, kurie būtų naudojami tik tame tinkle. Iš visų rezervuotų IP adresų centrinėje SIS II bus naudojamas nustatytas IP adresų, kurių nebus galima naudoti niekur kitur, rinkinys.

4.6.2. IPv6 palaikymas

Galima daryti prielaidą, kad valstybių narių vietiniuose tinkluose bus naudojamas TCP/IP protokolas. Tačiau vienose tinklavietėse gali būti naudojama 4 versija, o kitose – 6 versija. Tinklo prieigos taškai turėtų būti parengti taip, kad galėtų atlikti tinklų sietuvo funkciją, ir galėtų veikti nepriklausomai nuo centrinėje SIS II ir N.SIS II naudojamų tinklo protokolų.

4.6.3. Statinis maršrutas

Duomenims perduoti į valstybes nares CU ir BCU gali būti naudojamas vienas ir toks pat IP adresas. Todėl ryšių infrastruktūra turėtų leisti naudoti statinį maršrutą.

4.6.4. Užtikrinama duomenų srauto sparta

Tol, kol duomenų srauto sparta CU arba BCU yra mažesnė kaip 90 %, susijusi valstybė narė turi užtikrinti, kad dažnių juostos pločio rodiklis nuolatos bus 100 %.

4.6.5. Kitos specifikacijos

Tam, kad CS-SIS būtų palaikoma, ryšių infrastruktūra turi atitikti bent minimalias technines specifikacijas:

perdavimo delsa (įskaitant piko valandas) turi būti mažesnė kaip arba lygi 150 ms 95 % duomenų paketų ir mažesnė kaip 200 ms 100 % duomenų paketų.

Duomenų paketų praradimo tikimybė (įskaitant piko valandas) turi būti mažesnė kaip arba lygi 10^{-4} 95 % duomenų paketų ir mažesnė kaip 10^{-3} 100 % paketų.

Pirmiau minėtas specifikacijas turi atitikti kiekvienas atskiras prieigos taškas.

Tarp CU ir BCU perduodamų paketų delsa turi būti mažesnė kaip arba lygi 60 ms.

4.7. *Funkcinis atsparumas*

CS-SIS projekte numatytas didelio prieinamumo reikalavimas. Todėl siekiant apsisaugoti nuo įvairių komponentų veiklos sutrikimų visa įranga dubliuojama.

Ryšių infrastruktūros komponentai taip pat turi būti atsparūs gedimams. Gedimams turi būti atsparūs šie ryšių infrastruktūros komponentai:

— pagrindinis tinklas,

— maršruto parinkimo įtaisai,

— prisijungimo taškai (angl. *Points of Presence*),

— vietinių linijų jungtys (įskaitant atlikusius kabelius),

— saugumo priemonės (šifravimo priemonės, užkardos ir kt.),,

— visos bendrosios paslaugos (DNS, NTP ir kt.),

— LNI/BLNI.

Visi tinklo įrenginiai po gedimo turėtų persijungti automatiškai, operacijų neatliekant rankiniu būdu.

5. **Stebėsena**

Siekiant supaprastinti stebėseną, ryšių infrastruktūros stebėsenos priemonės turi būti tokios, kad jas būtų galima integruoti su institucijos, atsakingos už centrinės SIS II operatyvųjį valdymą, stebėsenos įrenginiais.

6. **Bendrosios paslaugos**

Be specialiojo tinklo ir apsaugos paslaugų ryšių infrastruktūra taip pat turi užtikrinti bendrąsias paslaugas.

Specialiosios paslaugos turi būti įdiegtos abiejuose sistemos centruose dėl su duomenų pertekliumi susijusių priežasčių.

Ryšių infrastruktūra turi užtikrinti toliau nurodytas neprivalomas bendrąsias paslaugas:

Paslauga	Papildoma informacija
DNS	Šiuo metu automatinis persijungimas iš CU į BCU tinklo gedimo atveju grindžiamas IP adreso pakeitimu bendrajame DNS serveryje.
E. pašto persiuntimo serveris	Bendras e. pašto persiuntimo serveris gali būti naudingas siekiant standartizuoti skirtingų valstybių narių e. pašto sąrankas ir, priešingai nei specialusis serveris, toks serveris nenaudoja jokių CU ir (arba) BCU tinklo išteklių. E. paštas, persiunčiamas naudojant bendrą e. pašto persiuntimo serverį, turi atitikti saugumo šabloną (angl. *security template*).
NTP	Ši paslauga gali būti naudojama tinklo įrenginių laikrodžiams sinchronizuoti.

7. **Prieinamumas**

CS-SIS ir LNI bei BLNI prieinamumo rodiklis 28 dienų nepertraukiamu laikotarpiu turi būti 99,99 %, neatsižvelgiant į tinklo prieinamumą.

Ryšių infrastruktūros prieinamumo rodiklis turi būti 99,99 %.

8. **Apsaugos priemonės**

8.1. *Tinklo šifravimas*

Centrinė SIS II neleidžia perduoti duomenų, kuriems taikomi dideli arba labai dideli apsaugos reikalavimai, už LAN ribų, jeigu jie nėra šifruoti. Reikėtų užtikrinti, kad tinklo teikėjas jokiu būdu negalėtų prieiti prie SIS II darbinių duomenų bei SIRENE duomenų, kuriais keičiamasi.

Siekiant aukšto apsaugos lygio, ryšių infrastruktūra turi sudaryti galimybę valdyti liudijimus ir (arba) raktus. Turi būti sudaryta galimybė vykdyti šifravimo įrenginių nuotolinį administravimą ir nuotolinę stebėseną. Šifravimo algoritmai turi atitikti bent šiuos reikalavimus:

— Simetriniai šifravimo algoritmai:

• 3DES (128 bitų) arba didesni,

• rakto generavimui turi būti naudojamas atsitiktinis dydis, kuris neleistų sumažinti rakto dydžio bandymo įsilaužti metu,

• šifravimo raktai arba informacija, kuri gali būti naudojama raktams gauti, turi būti saugomi tol, kol jie laikomi atmintyje.

— Asimetriniai šifravimo algoritmai:

• RSA (1 024 bitų modulis) arba didesnis,

• rakto generavimui turi būti naudojamas atsitiktinis dydis, kuris neleistų sumažinti rakto dydžio bandymo įsilaužti metu.

Naudojamas ESP (angl. *Encapsulated Security Payload*) protokolas (RFC2406). Jis naudojamas tuneliavimo režimu. Pagrindinė dalis ir originali IP antraštė turi būti šifruotos.

Siekiant apsikeisti sesijų raktais, naudojamas IKE (angl. *Internet Key Exchange*) protokolas.

IKE raktai galioja ne ilgiau kaip 1 dieną.

Sesijų raktai galioja ne ilgiau kaip 1 valandą.

8.2. *Kiti saugumo aspektai*

Ryšių infrastruktūra užtikrina ne tik SIS II prieigos taškų apsaugą, bet taip pat turi užtikrinti neprivalomų bendrųjų paslaugų apsaugą. Šioms paslaugoms turi būti taikomos tokios pačios apsaugos priemonės, kokios taikomos CS-SIS. Todėl visoms bendrosioms paslaugoms apsaugoti turi būti naudojamos bent šios priemonės: užkarda, antivirusinė programa ir įsilaužimo aptikimo sistema. Be to, bendrosioms paslaugoms teikti naudojami įrenginiai ir jų apsaugos priemonės turi būti nuolat stebimi (užsiregistravus ir atliekant tolesnius veiksmus) saugumo tikslais.

Siekiant, kad apsaugos lygis nuolatos būtų aukštas, institucija, atsakinga už centrinės SIS II operatyvųjį valdymą, turi žinoti apie visus saugumo pažeidimus ryšių infrastruktūroje. Todėl ryšių infrastruktūra turi sudaryti galimybę apie saugumo pažeidimus iš karto pranešti institucijai, atsakingai už centrinės SIS II operatyvųjį valdymą. Apie visus saugumo pažeidimus turi būti pranešama reguliariai, pvz., kas mėnesį, ir iš karto jiems įvykus.

9. **Pagalbos tarnyba ir palaikymo struktūra**

Ryšių infrastruktūros paslaugų teikėjas turi užtikrinti, kad veiktų pagalbos tarnyba, kuri bendrautų su institucija, atsakinga už centrinės SIS II operatyvųjį valdymą.

10. **Sąveika su kitomis sistemomis**

Ryšių infrastruktūra turi užtikrinti, kad informacija nebūtų perduota už nustatytų ryšio kanalų ribų, Įgyvendinant techniškai tai reiškia, kad:

— griežtai draudžiama bet kokia neteisėta ir (arba) nekontroliuojama prieiga prie kitų tinklų. taip pat prisijungimas prie interneto,

— duomenys neturi „nutekėti“ į kitas tinklo sistemas, pvz., draudžiama sujungti skirtingus IP VPN.

Be pirmiau minėtų techninių ribojimų, apribojimai taikomi ir ryšių infrastruktūros pagalbos tarnybai. Pagalbos tarnyba negali perduoti jokios su centrine SIS II susijusios informacijos jokiai kitai šaliai, išskyrus už centrinės SIS II operatyvųjį valdymą atsakingą instituciją.