II

(Tiesību akti, kas pieņemti, piemērojot EK/Euratom līgumus, un kuru publicēšana nav obligāta)

LĒMUMI

KOMISIJA

KOMISIJAS LĒMUMS

(2007. gada 16. marts)

par prasību noteikšanu Šengenas Informācijas sistēmas II tīklam (1. pīlārs)

(izziņots ar dokumenta numuru K(2007) 845)

(Autentisks ir tikai teksts bulgāru, čehu, franču, grieķu, holandiešu, igauņu, ungāru, itāliešu, latviešu, lietuviešu, maltiešu, poļu, portugāļu, rumāņu, slovāku, slovēņu, somu, spāņu, vācu un zviedru valodā)

(2007/170/EK)

EIROPAS KOPIENU KOMISIJA,

ņemot vērā Eiropas Kopienas dibināšanas līgumu,

ņemot vērā Padomes 2001. gada 6. decembra Regulu (EK) Nr. 2424/2001 par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izstrādi [1], un jo īpaši tās 4. panta a) apakšpunktu,

tā kā:

(1) Lai attīstītu *SIS II* ir vajadzīgs noteikt tehniskās specifikācijas attiecībā uz sakaru tīklu, tā komponentēm un īpašajām tīkla prasībām.

(2) Komisijai un dalībvalstīm jāveic attiecīgi pasākumi, jo īpaši attiecībā uz vienveidīgas valsts saskarnes elementiem.

(3) Šis lēmums neierobežo turpmāk pieņemtos Komisijas lēmumus par *SIS II* attīstību, jo īpaši par drošības prasību izstrādāšanu.

(4) Gan Regula (EK) Nr. 2424/2001, gan Padomes Lēmums 2001/886/TI [2] reglamentē *SIS II* izstrādi. Lai nodrošinātu, ka *SIS II* tiek izveidota vienā īstenošanas procesā, šā lēmuma noteikumiem jāatspoguļo Komisijas lēmuma noteikumi par prasību noteikšanu *SIS II* tīklam, kas jāievēro, izpildot Lēmumu 2001/886/TI.

(5) Apvienotā Karaliste saskaņā ar Padomes 2000. gada 29. maija Lēmumu 2000/365/EK par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā [3] nepiedalījās Regulas (EK) Nr. 2424/2001 pieņemšanā, un minētā regula tai nav saistoša un nav jāpiemēro, jo tā papildina Šengenas *acquis* noteikumus. Tādēļ šis Komisijas lēmums neattiecas uz Apvienoto Karalisti.

(6) Īrija saskaņā ar Padomes 2002. gada 28. februāra Lēmumu 2002/192/EK par Īrijas lūgumu piedalīties dažu Šengenas *acquis* noteikumu īstenošanā [4] nepiedalījās Regulas (EK) Nr. 2424/2001 pieņemšanā, minētā regula tai nav saistoša un nav jāpiemēro, jo tā papildina Šengenas *acquis* noteikumus. Tādēļ šis Komisijas lēmums neattiecas uz Īriju.

[1] OV L 328, 13.12.2001., 4. lpp. Regulā grozījumi izdarīti ar Regulu (EK) Nr. 1988/2006 (OV L 411, 30.12.2006., 1. lpp.).

[2] OV L 328, 13.12.2001., 1. lpp.

[3] OV L 131, 1.6.2000., 43. lpp. Lēmumā grozījumi izdarīti ar Lēmumu 2004/926/EK (OV L 395, 31.12.2004., 70. lpp.).

[4] OV L 64, 7.3.2002., 20. lpp.

(7) Saskaņā ar 5. pantu Līgumam par Eiropas Savienību un Eiropas Kopienas dibināšanas līgumam pievienotajā Protokolā par Dānijas nostāju Dānija ir nolēmusi transponēt Padomes Regulu (EK) Nr. 2424/2001 Dānijas tiesību aktos. Tādējādi saskaņā ar starptautiskajām tiesībām Regula (EK) Nr. 2424/2001 Dānijai ir saistoša.

(8) Attiecībā uz Islandi un Norvēģiju Regula (EK) Nr. 2424/2001 un Lēmums 2001/886/TI papildina Šengenas *acquis* noteikumus tā nolīguma nozīmē, ko Eiropas Savienības Padome, Islandes Republika un Norvēģijas Karaliste noslēgusi par abu minēto valstu iesaistīšanos Šengenas *acquis* īstenošanā, piemērošanā un izstrādē jomā [1], kas minēta 1. panta B punktā Padomes 1999. gada 17. maija Lēmumā 1999/437/EK par dažiem pasākumiem, lai piemērotu Eiropas Savienības Padomes, Islandes Republikas un Norvēģijas Karalistes Nolīgumu par abu minēto valstu iesaistīšanos Šengenas *acquis* īstenošanā, piemērošanā un izstrādē [2].

(9) Attiecībā uz Šveici Regula (EK) Nr. 2424/2001 un Lēmums 2001/886/TI papildina Šengenas *acquis* tā nolīguma nozīmē, ko Eiropas Savienība, Eiropas Kopiena un Šveices Konfederācija noslēgusi par šīs valsts iesaistīšanos Šengenas *acquis* īstenošanā, piemērošanā un izstrādē jomā, kas minēta 4. panta 1. punktā Padomes lēmumā par šā nolīguma parakstīšanu Kopienas vārdā un dažu šā nolīguma noteikumu provizorisku piemērošanu.

(10) Šis lēmums ir dokuments, kura pamatā ir Šengenas *acquis* vai kas ir ar to citādi saistīts Pievienošanās akta 3. panta 1. punkta nozīmē.

(11) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota saskaņā ar Regulas (EK) Nr. 2424/2001 6. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

SIS II sakaru infrastruktūras sistēmas arhitektūras projekta tehniskās specifikācijas jānosaka pielikumā.

2. pants

Šis lēmums ir adresēts Beļģijas Karalistei, Bulgārijas Republikai, Rumānijai, Čehijas Republikai, Vācijas Federatīvajai Republikai, Igaunijas Republikai, Grieķijas Republikai, Spānijas Karalistei, Francijas Republikai, Itālijas Republikai, Kipras Republikai, Latvijas Republikai, Lietuvas Republikai, Luksemburgas Lielhercogistei, Ungārijas Republikai, Maltas Republikai, Nīderlandes Karalistei, Austrijas Republikai, Polijas Republikai, Portugāles Republikai, Slovēnijas Republikai, Slovākijas Republikai, Somijas Republikai un Zviedrijas Karalistei.

Briselē, 2007. gada 16. martā

Komisijas vārdā —
priekšsēdētāja vietnieks
Franco FRATTINI

[1] OV L 176, 10.7.1999., 36. lpp.
[2] OV L 176, 10.7.1999., 31. lpp.

PIELIKUMS

SATURA RĀDĪTĀJS

1. **Ievads**

Šajā dokumentā ir dota sīkāka informācija par sakaru tīkla uzbūvi, ietvertām komponentēm un īpašām tīkla prasībām.

1.1. *Akronīmi un saīsinājumi*

Šajā iedaļā ir paskaidroti dokumentā izmantotie akronīmi.

Akronīmi un saīsinājumi	Skaidrojums
BLNI	*Backup Local National Interface* (Vietējas valsts saskarnes dublējums)
CEP	*Central End Point* (Centrālais galapunkts)
CNI	*Central National Interface* (Centrālā valsts saskarne)
CS	*Central System* (Centrālā sistēma)
CS-SIS	*Technical support function containing the SIS II database* (Tehniskā atbalsta funkcija, kas ietver *SIS II* datubāzi)
DNS	*Domain Name Server* (Domēnu vārdu serveris)
FCIP	*Fibre Channel over IP* (Optiskās šķiedras kanāls ar interneta protokolu)
FTP	*File Transport Protocol* (Datņu pārsūtīšanas protokols)
HTTP	*Hyper Text Transfer Protocol* (Hiperteksta transporta protokols)
IP	*Internet Protocol* (Interneta protokols)
LAN	*Local Area Network* (Lokālais tīkls)
LNI	*Local National Interface* (Vietējā valsts saskarne)
Mbps	*Megabits per second* (Megabiti sekundē)
MDC	*Main Developer Contractor*
N.SIS II	*The national section in each Member State* (Valsts nodaļa katrā dalībvalstī)
NI-SIS	*A uniform national interface* (Vienveidīga valsts saskarne)
NTP	*Network Time Protocol* (Tīkla laika protokols)
SAN	*Storage Area Network* (Atmiņas apgabalu tīkls)
SDH	*Synchronous Digital Hierarchy* (Sinhronā ciparhierarhija)
SIS II	*Schengen Information System, second generation* (Otrās paaudzes Šengenas Informācijas sistēma)
SMTP	*Simple Mail Transport Protocol* (Vienkāršais pasta pārsūtīšanas protokols)
SNMP	*Simple Network Management Protocol* (Vienkāršais tīkla pārvaldības protokols)
s-TESTA	*Secure Trans-European Services for Telematics between Administrations* (Tīkls drošiem Eiropas pakalpojumiem telemātikai starp iestādēm) ir *IDABC* programmas pasākums (Visei-ropas elektroniskās pārvaldības pakalpojumu savietojamības nodrošināšana valsts pārvaldes iestādēm, uzņēmumiem un pilsoņiem. Eiropas Parlamenta un Padomes 2004. gada 21. aprīļa Lēmums 2004/387/EK).
TCP	*Transmission Control Protocol* (Pārraides vadības protokols)
VIS	*Visa Information System* (Vīzu informācijas sistēma)
VPN	*Virtual Private Network* (Virtuāls privātais tīkls)
WAN	*Wide Area Network* (Teritoriālais tīkls)

2. **Vispārīgs pārskats**

SIS II ietver šādus elementus.

— Centrālā sistēma (turpmāk – "centrālā *SIS II*"), kas ietver:

  • tehniskā atbalsta funkciju (turpmāk – "*CS-SIS*"), kas ietver *SIS II* datubāzi. Galvenā *CS-SIS* veic tehnisko uzraudzību un vadību, un dublējošā *CS-SIS* nodrošina galvenās *CS-SIS* darbību kļūdas gadījumā;

  • vienveidīgu valsts saskarni (turpmāk – "*NI-SIS*"),

— Valsts nodaļa (turpmāk – "*N.SIS II*") katrā dalībvalstī, kas ietver valsts datu sistēmas, kuras ir savienotas ar centrālo *SIS II*. *N.SIS II* var ietvert datu datni (turpmāk – "valsts kopija"), kurā ir ietverta pilnīga vai daļēja *SIS II* datubāzes kopija.

— Sakaru infrastruktūra starp *CS-SIS* un *NI-SIS* (turpmāk – "sakaru infrastruktūra"), ar ko nodrošina šifrētu virtuālu tīklu *SIS II* datiem un datu apmaiņai starp *SIRENE* birojiem.

NI-SIS ietver šādus elementus.

— Viena vietējā valsts saskarne (turpmāk – "*LNI*") katrā dalībvalstī, kas ir saskarne, ar kuru dalībvalsts fiziski pieslēdzas drošam sakaru tīklam un tā ietver šifrēšanas ierīces, kas paredzētas *SIS II* un *SIRENE* datu plūsmai. *LNI* atrodas dalībvalstī.

— Alternatīvs vietējas valsts saskarnes dublējums (turpmāk – "*BLNI*"), kas ietver tieši to pašu un kam ir tieši tāda pati funkcija kā *LNI*.

LNI un *BLNI* izmanto tikai *SIS II* sistēma un vienīgi *SIRENE* informācijas apmaiņas vajadzībām. Ar katru dalībvalsti tiks noteikta un saskaņota *LNI* un *BLNI* īpašā konfigurācija, lai ņemtu vērā drošības prasības, fizisko izvietojumu un instalēšanas nosacījumus, ieskaitot tīkla operatora pakalpojuma sniegšanu, lai fiziskais *s-TESTA* savienojums varētu ietvert vairākus *VPN* kanālus citām sistēmām, piemēram, *VIS* un *Eurodac*.

— Centrālā valsts saskarne (turpmāk – "*CNI*") ir lietojumprogramma, kura nodrošina piekļuvi *CS-SIS*. Katrai dalībvalstij ir atsevišķi loģiskie piekļuves punkti *CNI*; tiek izmantots centrālais ugunsmūris.

Sakaru infrastruktūra starp *CS-SIS* un *NI-SIS* ietver šādu elementu.

— Tīkls drošiem Eiropas pakalpojumiem telemātikai starp iestādēm (turpmāk – *s-TESTA*), ar ko nodrošina šifrētu, virtuālu, privātu tīklu, kas paredzētas *SIS II* un *SIRENE* datu plūsmai.

3. **Ģeogrāfiskā aptveramība**

Sakaru infrastruktūrai jāspēj aptvert un sniegt vajadzīgos pakalpojumus visām dalībvalstīm.

Tās ir visas ES dalībvalstis (Beļģija, Francija, Vācija, Luksemburga, Nīderlande, Itālija, Portugāle, Spānija, Grieķija, Austrija, Dānija, Somija, Zviedrija, Kipra, Čehija, Igaunija, Ungārija, Latvija, Lietuva, Malta, Polija, Slovākija, Slovēnija, Apvienotā Karaliste un Īrija) + Norvēģija, Islande, Šveice.

Turklāt jānodrošina aptveramība jaunajām dalībvalstīm Rumānijai un Bulgārijai.

Visbeidzot, sakaru infrastruktūru jāvar paplašināt tā, lai centrālai *SIS II* varētu piekļūt no jebkuras citas valsts vai iestādes (piemēram Eiropols, *Eurojust*).

4. **Tīkla pakalpojumi**

Visur, kur ir minēts protokols vai arhitektūra, jāņem vērā, ka ir pieņemamas arī līdzvērtīgas nākotnes tehnoloģijas, protokoli un arhitektūra.

4.1. *Tīkla izkārtojums*

SIS II arhitektūra izmanto centralizētos pakalpojumus, kuriem var piekļūt no dažādām dalībvalstīm. Stabilitātes nodrošināšanai šie centralizētie pakalpojumi tiek dublēti divas dažādās vietās, t.i., Strasbūrā Francijā un *St Johann im Pongau* Austrijā attiecīgi *CS-SIS*, *CU* un dublējošā *CS-SIS*, *BCU*.

Centrālām vienībām – galvenām un dublētām – jābūt pieejamām no dažādām dalībvalstīm. Iesaistītajām valstīm var būt vairāki tīkla piekļuves punkti (*LNI* un *BLNI*), lai savstarpēji savienotu savas valsts sistēmas ar centrāliem pakalpojumiem.

Neatkarīgi no galvenā savienojuma ar centrāliem pakalpojumiem, sakaru infrastruktūrai ir arī jāatbalsta divpusēja papildu informācijas apmaiņa starp *SIRENE* birojiem dažādās dalībvalstīs.

4.2. *Savienojuma veids galvenā CS-SIS – dublējošā CS-SIS*

Vajadzīgais savienojuma veids starp galveno *CS-SIS* un dublējošo *CS-SIS* ir *SDH* gredzens vai līdzvērtīga jauna nākotnes arhitektūra un tehnoloģija. *SDH* infrastruktūra tiks izmantota, lai paplašinātu abu centrālo vienību esošos tīklus un izveidotu vienotu *LAN*. Minēto *LAN* lietos, lai nodrošinātu nepārtrauktu datu sinhronizāciju starp *CU* un *BCU*.

4.3. *Joslas platums*

Sakaru infrastruktūras būtiska prasība ir joslas platuma lielums, ko tā var piešķirt dažādām savstarpēji savienotām vietnēm, un tās spēja atbalstīt minēto joslas platumu savā pamattīklā.

Joslas platums, kas vajadzīgs *LNI* un alternatīvai *BLNI*, būs atšķirīgs katrai dalībvalstij atkarībā no izvēles lietot valsts kopijas, centrālo meklēšanu un biometrisko datu apmaiņu.

Faktiskie joslas platuma rādītāji, ko sakaru infrastruktūra izlemj piedāvāt, nav atbilstīgi, ja tie neatbilst dalībvalstu minimālām vajadzībām.

Jebkuras šādas iepriekšminētās vietnes var pārsūtīt milzīgus datu apjomus (burtu un ciparu datus, biometriskus datus vai dokumentus) abos virzienos. Tāpēc sakaru infrastruktūrai jānodrošina pietiekams minimālais garantētais augšupielādes un lejupielādes ātrums katram savienojumam.

Sakaru infrastruktūrai jāpiedāvā savienojumi, kas atbilst ātrumam no 2 *Mbps* līdz 155 *Mbps* vai ātrākam. Tīklam jānodrošina pietiekams minimālais garantētais augšupielādes un lejupielādes ātrums visiem savienojumiem, un tam jābūt pietiekami lielam, lai atbalstītu tīkla piekļuves punktu kopējo joslas platumu.

4.4. *Servisa klases*

Centrālā *SIS II* atbalstīs pieprasījumu/brīdinājumu prioritizācijas iespēju. Saskaņā ar atvasinātu prasību sakaru infrastruktūrai būs jāatbalsta iespēja prioritizēt datu plūsmas.

Ir pieņemts, ka tīkla prioritizācijas parametrus nosaka centrālā *SIS II* visām paketēm, kurām tas ir vajadzīgs. Tiks izmantots *Weighted Fair Queuing*. Tas nozīmē, ka sakaru infrastruktūrai jāspēj pārņemt datu paketēm pirmsākuma *LAN* noteikto prioritizāciju un attiecīgi jāsaglabā šī prioritizācija savā pamattīklā. Turklāt attālajā vietnē (*remote site*) sakaru infrastruktūrai jāpiegādā sākotnējās paketes, ievērojot to pašu prioritizāciju, kas tika noteikta pirmsākuma *LAN*.

4.5. *Atbalstītie protokoli*

Centrālā *SIS II* izmantos dažādus tīklu saziņas protokolus. Sakaru infrastruktūrai jāatbalsta daudzi un dažādi tīklu saziņas protokoli. Atbalstāmie standarta protokoli ir *HTTP*, *FTP*, *NTP*, *SMTP*, *SNMP* un *DNS*.

Papildus standarta protokoliem sakaru infrastruktūrai jāspēj uzturēt dažādus tunelēšanas protokolus, *SAN* replicēšanas protokolus un *BEA WebLogic proprietary Java-to-Java* savienojuma protokolus. Tunelēšanas protokoli (piem., *IPsec* tuneļa režīmā) tiks izmantoti, lai pārsūtītu šifrētu datu plūsmu uz galamērķi.

4.6. *Tehniskās specifikācijas*

4.6.1. *IP adresēšana (IP addressing)*

Sakaru infrastruktūrai jārezervē virkni *IP* adrešu, kuras var izmantot vienīgi tīkla iekšienē. Rezervēto *IP* adrešu ietvaros centrālā *SIS II* izmantos atvēlēto *IP* adrešu komplektu, kuras netiks izmantotas nekur citur.

4.6.2. *IPv6* atbalsts

Var pieņemt, ka dalībvalstu vietējā tīklā izmantotais protokols būs *TCP/IP*. Tomēr dažas vietnes būs balstītas uz 4. versiju, bet citas – uz 6. versiju. Tīkla piekļuves punktiem jābūt iespējai darboties kā vārtejai, un tiem jāspēj darboties neatkarīgi no tīkla protokoliem, kas tiek izmantoti centrālajā *SIS II*, kā arī *N.SIS II*.

4.6.3. Statiskā maršruta ievade (*Static Route Injection*)

CU un *BCU* var izmantot vienu un identisku *IP* adresi saziņai ar dalībvalstīm. Tādēļ sakaru infrastruktūrai jāatbalsta statiskā maršruta ievade.

4.6.4. Pastāvīgās plūsmas likme (*Sustained Flow Rate*)

Tā kā *CU* vai *BCU* savienojuma noslodzes likme ir mazāka par 90 %, konkrētai dalībvalstij jāspēj pastāvīgi uzturēt 100 % no tās noteiktās joslas platuma.

4.6.5. Citas specifikācijas

CS-SIS atbalsta vajadzībām sakaru infrastruktūrai jāatbilst vismaz tehnisko specifikāciju minimālām prasībām.

Tranzīta kavējumam (tai skaitā sastrēguma stundās) jābūt mazākam vai vienādam ar 150 ms attiecībā uz 95 % pakešu un mazākam par 200 ms attiecībā uz 100 % pakešu.

Paketes pazaudēšanas iespējamībai (tai skaitā sastrēguma stundās) jābūt mazākai vai vienādai ar to 10^{-4} attiecībā uz 95 % pakešu un mazākai par 10^{-3} attiecībā uz 100 % pakešu.

Iepriekšminētās specifikācijas jāparedz katram piekļuves punktam atsevišķi.

Savienojuma starp *CU* un *BCU* aprites kavējumam jābūt mazākam vai vienādam ar 60 ms.

4.7. *Sistēmas stabilitāte*

Kā prasība *CS-SIS* ir paredzēts ar lielu piekļuves kapacitāti. Šim nolūkam, dublējot visas iekārtas, sistēmā ir nodrošināta stabilitāte komponenšu disfunkcijas gadījumā.

Sakaru infrastruktūras komponentiem jābūt nodrošinātiem arī pret komponenšu kļūdām. Attiecībā uz sakaru infrastruktūru tas nozīmē, ka jānodrošina stabilitāte šādām komponentēm:

— pamattīkls (*backbone network*),

— maršrutēšanas ierīces (*routing devices*),

— klātbūtnes punkti (*Points of Presence*),

— abonentlīnijas pieslēgumi (*local loop connections*) (ieskaitot rezerves kabeļu ievilkšanu),

— drošības ierīces (*security devices*) (šifrēšanas ierīces, ugunsmūri u.c.),

— visi pamatpakalpojumi (*generic services*) (*DNS, NTP* u.c.),

— *LNI/BLNI*.

Kļūmpārlēces mehānismiem visās tīkla iekārtās jāiedarbojas bez manuālas iejaukšanās.

5. **Uzraudzība**

Lai atvieglotu uzraudzību, jābūt iespējai integrēt sakaru infrastruktūras uzraudzības līdzekļus ar uzraudzības līdzekļiem, kas ir tās organizācijas rīcībā, kas atbild par centrālās *SIS II* darbības vadību.

6. **Pamatpakalpojumi**

Neatkarīgi no atvēlētā tīkla un drošības pakalpojumiem sakaru infrastruktūrai jāpiedāvā arī pamatpakalpojumi.

Attiecīgie pakalpojumi stabilitātes nolūkos jāizpilda abās centrālās vienībās.

Sakaru infrastruktūrā jābūt pieejamiem šādiem izvēles pamatpakalpojumiem.

Pakalpojums	Papildu informācija
DNS	Pašreiz kļūmjpārlēces procedūra, lai pārslēgtos no *CU* uz *BCU* tīkla kļūdas gadījumā, ir balstīta uz *IP* adreses maiņu pamata *DNS* serverī.
E-mail relay	*Generic e-mail relay* izmantošana varētu būt lietderīga e-pasta iestatījumiem dažādām dalībvalstīm un, pretēji atvēlētam serverim, neizmanto tīkla resursus no *CU/BCU*. Arī e-pastiem, kuriem izmanto *generic e-mail relay*, jāatbilst drošības noteikumiem.
NTP	Šo pakalpojumu var izmantot, lai saskaņotu tīkla iekārtu pulksteņus.

7. **Piekļuves kapacitāte**

CS-SIS un *LNI*, un *BLNI* jāspēj nodrošināt 99,99 % piekļuves kapacitāti 28 dienu darbības periodā, neskaitot piekļūšanas spēju tīklam.

Sakaru infrastruktūras piekļuves kapacitātei jābūt 99,99 %.

8. **Drošības pakalpojumi**

8.1. *Tīkla šifrēšana*

Centrālā *SIS II* neatļauj pārsūtīt datus, uz kuriem attiecas augstas vai ļoti augstas aizsardzības prasības, ārpus *LAN* bez šifrēšanas. Jānodrošina, ka tīkla operatoram nekādā gadījumā nebūs pieejas *SIS II* darbības datiem, kā arī attiecīgām *SIRENE* datu apmaiņām.

Lai uzturētu augstu drošības līmeni, sakaru infrastruktūrai jāatļauj pārvaldīt sertifikātus/atslēgas. Jābūt iespējamai šifrēšanas logu attālai pārvaldībai un attālai uzraudzībai. Šifrēšanas algoritmiem jāatbilst vismaz šādām prasībām.

— Simetriskās šifrēšanas algoritmi:

• *3DES (128 bits)* vai labāks,

• atslēgas ģeneratora darbības pamatā jābūt nejaušai vērtībai, kas neatļauj atslēgas saīsināšanu uzbrukuma gadījumā,

• šifrēšanas atslēgas vai informācija, ko var izmantot atslēgu iegūšanai, vienmēr tiek aizsargātas.

— Asimetriskās šifrēšanas algoritmi:

• *RSA (1 024 bit modulus*) vai labāks,

• atslēgas ģeneratora darbības pamatā jābūt nejaušai vērtībai, kas neatļauj atslēgas saīsināšanu uzbrukuma gadījumā.

Ir jāizmanto *Encapsulated Security Payload (ESP, RFC2406*) protokols. Tas jāpielieto tuneļa režīmā. Ir jāšifrē *Payload* un oriģinālā *IP*-iesākums.

Sesijas atslēgu apmaiņai jāizmanto *Internet Key Exchange* (*IKE*) protokols.

IKE atslēgas nevar būt spēkā ilgāk kā 1 dienu.

Sesijas atslēgas nevar būt spēkā ilgāk kā 1 dienu.

8.2. *Citi aizsardzības elementi*

Bez *SIS II* piekļuves punktu aizsardzības sakaru infrastruktūrai jāaizsargā arī izvēles pamatpakalpojumi. Šiem pakalpojumiem arī jāpiemēro tie paši aizsardzības pasākumi, kas *CS-SIS*. Tāpēc visi pamatpakalpojumi jāaizsargā vismaz ar ugunsmūri, pretvīrusu programmu un ielaušanās atklāšanas sistēmu. Turklāt pamatpakalpojumu iekārtām un to aizsardzības pasākumiem jāveic pastāvīga uzraudzība (reģistrēšana un sekojums).

Augsta aizsardzības līmeņa uzturēšanas vajadzībām par centrālās *SIS II* darbības vadību atbildīgajai organizācijai jābūt informētai par jebkādiem ar drošību saistītiem starpgadījumiem, kas notiek sakaru infrastruktūrā. Tāpēc sakaru infrastruktūrai jāatļauj nekavējoties ziņot par visiem svarīgākajiem ar drošību saistītiem starpgadījumiem organizācijai, kas atbild par centrālās *SIS II* darbības vadību. Par visiem ar drošību saistītiem starpgadījumiem jāziņo regulāri, piemēram, katru mēnesi un īpašos gadījumos.

9. **Palīdzības dienests un atbalsta struktūra**

Sakaru infrastruktūras pakalpojuma sniedzējam jānodrošina palīdzības dienesta pakalpojumi, kurš sadarbojas ar organizāciju, kas atbild par centrālās *SIS II* darbības vadību.

10. **Mijiedarbība ar citām sistēmām**

Sakaru infrastruktūrai jānodrošina, ka informācija nevar nokļūt ārpus piešķirtajiem sakaru kanāliem. Attiecībā uz tehnisko izpildi tas nozīmē, ka:

— ir aizliegta jebkāda nesankcionēta un/vai nekontrolēta piekļuve. Tas attiecas arī uz mijiedarbību ar tīmekli;

— nedrīkst notikt datu noplūde uz citām sistēmām tīklā, piemēram, nav atļauta dažādu *IP VPN* mijiedarbība.

Neatkarīgi no iepriekšminētajiem tehniskajiem ierobežojumiem, tas attiecas arī uz sakaru infrastruktūras palīdzības dienestu. Palīdzības dienests nevar nodot nekādu informāciju saistībā ar centrālo *SIS II* kādai citai pusei, kā tikai tai, kas ir atbildīga par centrālās *SIS II* darbības vadību.