KOMISSION PÄÄTÖS,

tehty 16 päivänä maaliskuuta 2007,

toisen sukupolven Schengenin tietojärjestelmää (SIS II) koskevista verkonhallinnan vaatimuksista (kolmas pilari)

(2007/171/EY)

EUROOPAN YHTEISÖJEN KOMISSIO, joka

ottaa huomioon Euroopan unionista tehdyn sopimuksen,

ottaa huomioon toisen sukupolven Schengenin tietojärjestelmän (SIS II) kehittämisestä 6 päivänä joulukuuta 2001 tehdyn neuvoston päätöksen 2001/886/YOS [1] ja erityisesti sen 4 artiklan a alakohdan,

sekä katsoo seuraavaa:

(1) Toisen sukupolven Schengenin tietojärjestelmän (SIS II) kehittämistä varten on tarpeen vahvistaa tekniset vaatimukset järjestelmän tietoliikenneverkkoa ja sen osia sekä järjestelmään liittyvää verkonhallintaa varten.

(2) Tarvittavista järjestelyistä olisi sovittava komission ja jäsenvaltioiden kesken erityisesti siltä osin kuin ne koskevat jäsenvaltioissa sijaitsevia yhdenmukaisia kansallisia liittymiä.

(3) Tämä päätös ei estä komissiota tekemästä myöhemmin päätöksiä SIS II:n ja erityisesti tietoturvavaatimusten kehittämisestä.

(4) SIS II:n kehittämistä säännellään sekä neuvoston asetuksella (EY) N:o 2424/2001 [2] että päätöksellä 2001/886/YOS. Jotta voidaan varmistaa, että SIS II:n kehittämisen täytäntöönpano on kaikilta osin yhdenmukaista, tämän päätöksen säännösten tulee vastata sen SIS II:ta koskevista verkonhallinnan vaatimuksista tehtävän komission päätöksen säännöksiä, joka tehdään asetusta (EY) N:o 2424/2001 soveltaen.

(5) Yhdistynyt kuningaskunta osallistuu tähän päätökseen Euroopan unionista tehtyyn sopimukseen ja EY:n perustamissopimukseen liitetyn, Schengenin säännöstön sisällyttämisestä osaksi Euroopan unionia tehdyn pöytäkirjan 5 artiklan ja Ison-Britannian ja Pohjois-Irlannin yhdistyneen kuningaskunnan pyynnöstä saada osallistua joihinkin Schengenin säännöstön määräyksiin 29 päivänä toukokuuta 2000 tehdyn neuvoston päätöksen 2000/365/EY [3] 8 artiklan 2 kohdan mukaisesti.

(6) Irlanti osallistuu tähän päätökseen Euroopan unionista tehtyyn sopimukseen ja EY:n perustamissopimukseen liitetyn, Schengenin säännöstön sisällyttämisestä osaksi Euroopan unionia tehdyn pöytäkirjan 5 artiklan ja Irlannin pyynnöstä saada osallistua joihinkin Schengenin säännöstön määräyksiin 28 päivänä helmikuuta 2002 tehdyn neuvoston päätöksen 2002/192/EY [4] 5 artiklan 1 kohdan ja 6 artiklan 2 kohdan mukaisesti.

(7) Islannin ja Norjan osalta tällä päätöksellä kehitetään Schengenin säännöstön määräyksiä tietyistä Euroopan unionin neuvoston, Islannin tasavallan ja Norjan kuningaskunnan välillä viimeksi mainittujen osallistumisesta Schengenin säännöstön täytäntöönpanoon, soveltamiseen ja kehittämiseen tehdyn sopimuksen mukaisesti aloilla, joita tarkoitetaan tietyistä kyseisen sopimuksen yksityiskohtaisista soveltamissäännöistä tehdyn neuvoston päätöksen 1999/437/EY [5] 1 artiklan G alakohdassa.

(8) Sveitsin osalta tällä päätöksellä kehitetään Schengenin säännöstön määräyksiä Euroopan unionin, Euroopan yhteisön ja Sveitsin valaliiton välillä Sveitsin valaliiton osallistumisesta Schengenin säännöstön täytäntöönpanoon, soveltamiseen ja kehittämiseen tehdyn sopimuksen mukaisesti aloilla, joita tarkoitetaan neuvoston päätöksen 1999/437/EY 1 artiklan G alakohdassa sekä mainitun sopimuksen allekirjoittamisesta Euroopan yhteisön puolesta sekä sopimuksen tiettyjen määräysten väliaikaisesta soveltamisesta tehdyn neuvoston päätöksen 2004/849/EY [6] 4 artiklan 1 kohdassa.

(9) Tämä päätös on liittymisasiakirjan 3 artiklan 1 kohdassa tarkoitettu Schengenin säännöstöä kehittävä tai muuten siihen liittyvä säädös.

(10) Tässä päätöksessä säädetyt toimenpiteet ovat päätöksen 2001/886/YOS 5 artiklan 1 kohdalla perustetun komitean lausunnon mukaiset,

---

[1] EYVL L 328, 13.12.2001, s. 1.
[2] EYVL L 328, 13.12.2001, s. 4. Asetus sellaisena kuin se on muutettuna asetuksella (EY) N:o 1988/2006 (EUVL L 411, 30.12.2006, s. 1).
[3] EYVL L 131, 1.6.2000, s. 43. Päätös sellaisena kuin se on muutettuna päätöksellä 2004/926/EY (EUVL L 395, 31.12.2004, s. 70).
[4] EYVL L 64, 7.3.2002, s. 20.
[5] EYVL L 176, 10.7.1999, s. 31.
[6] EUVL L 368, 15.12.2004, s. 26.

ON PÄÄTTÄNYT SEURAAVAA:

Ainoa artikla

Tämän päätöksen liitteessä vahvistetaan tekniset eritelmät toisen sukupolven Schengenin tietojärjestelmän (SIS II) viestintäinfrastruktuurin fyysisen arkkitehtuurin suunnittelua varten.

Tehty Brysselissä 16 päivänä maaliskuuta 2007.

Komission puolesta
Franco FRATTINI
Varapuheenjohtaja

LIITE

SISÄLLYSLUETTELO

1. **Johdanto**

Tässä asiakirjassa käsitellään tietoliikenneverkon ja sen osien sekä järjestelmän verkonhallintaa koskevien vaatimusten rakennetta.

1.1 *Lyhytnimet ja lyhenteet*

Tässä jaksossa selitetään asiakirjassa käytetyt lyhytnimet ja lyhenteet.

Lyhytnimet ja lyhenteet	Selitys
BLNI	kansallisen paikallisliittymän varmuusjärjestelmä (Backup Local National Interface)
CEP	keskuspiste (Central End Point)
CNI	kansallinen keskusliittymä (Central National Interface)
CS	keskusjärjestelmä (Central System)
CS-SIS	tekninen tukitoiminto, joka sisältää SIS II -tietokannan
DNS	nimipalvelin (Domain Name Server)
FCIP	tekniikka, jonka avulla yhdistetään tallennusverkkoja IP:n avulla (Fibre Channel over IP)
FTP	tiedostonsiirtoprotokolla (File Transport Protocol)
HTTP	hypertekstin siirtoprotokolla (Hyper Text Transfer Protocol)
IP	Internet-protokolla
LAN	lähiverkko (Local Area Network)
LNI	kansallinen paikallisliittymä (Local National Interface)
Mbps	Mb/s (megabittiä sekunnissa)
MDC	järjestelmän pääkehittäjä (Main Developer Contractor)
N.SIS II	kunkin jäsenvaltion kansallinen järjestelmä
NI-SIS	yhdenmukainen kansallinen liittymä
NTP	NTP-protokolla (Network Time Protocol)
SAN	tallennusverkko (Storage Area Network)
SDH	synkroninen digitaalinen hierarkia
SIS II	toisen sukupolven Schengenin tietojärjestelmä
SMTP	SMTP-protokolla (Simple Mail Transport Protocol)
SNMP	SNMP-protokolla (Simple Network Management Protocol)
s-TESTA	hallintoelinten yhteinen suojattu yleiseurooppalainen telematiikkaverkko (Secure Trans-European Services for Telematics between Administrations), liittyy IDABC-ohjelmaan (yleiseurooppalaisten sähköisten viranomaispalveluiden yhteentoimiva toimittaminen julkishallinnolle, yrityksille ja kansalaisille). Euroopan parlamentin ja neuvoston päätös 2004/387/EY, tehty 21.4.2004.
TCP	tiedonsiirtoprotokolla (Transmission Control Protocol)
VIS	viisumitietojärjestelmä
VPN	virtuaalinen erillisverkko (Virtual Private Network)
WAN	suuralueverkko, esim. maiden välillä (Wide Area Network)

2. **Yleiskatsaus**

SIS II muodostuu seuraavista osista:

— keskustietokanta, jäljempänä 'SIS II:n keskustietojärjestelmä', joka muodostuu seuraavista osista:

  • tekninen tukitoiminto, jäljempänä 'CS-SIS', joka sisältää SIS II -tietokannan. CS-SIS-pääjärjestelmä huolehtii teknisestä valvonnasta ja hallinnoinnista, ja sen kaikki toiminnot turvataan toimintahäiriöiden varalta CS-SIS-varmuusjärjestelmän avulla,

  • yhdenmukaiset kansalliset liittymät, jäljempänä 'NI-SIS'.

— eri jäsenvaltioiden kansalliset järjestelmät, jäljempänä 'N.SIS II', jotka muodostuvat SIS II:n keskusjärjestelmän kanssa yhteydessä olevista kansallisista tietojärjestelmistä. N.SIS II voi sisältää tiedoston, jäljempänä 'kansallinen tiedosto', joka sisältää täydellisen tai osittaisen kopion SIS II -tietokannasta;

— CS-SIS:n ja NI-SIS:ien välinen viestintäinfrastruktuuri, jäljempänä 'viestintäinfrastruktuuri', eli suojattu virtuaaliverkko, joka sisältää SIS II -tiedot ja jonka välityksellä SIRENE-toimistot vaihtavat tietoja keskenään.

Kansalliset järjestelmät (NI-SIS) muodostuvat seuraavista osista:

— kussakin jäsenvaltiossa on yksi kansallinen paikallisliittymä, jäljempänä 'LNI', jonka kautta jäsenvaltio on fyysisesti yhteydessä suojattuun tietoliikenneverkkoon ja joka sisältää SIS II -järjestelmän ja SIRENE-tietojenvaihdon edellyttämät salausvälineet. LNI sijaitsee jäsenvaltion omistamissa tiloissa.

— valinnaisena kansallisen paikallisliittymän varmuusjärjestelmä, jäljempänä 'BLNI', jolla on täsmälleen sama sisältö ja toiminnot kuin LNI:llä.

LNI ja BLNI on tarkoitettu käytettäväksi yksinomaan SIS II -tietojärjestelmää ja SIRENE-toimistojen tietojenvaihtoa varten. LNI- ja BLNI-järjestelmien tekniset ominaisuudet täsmennetään ja niistä sovitaan kunkin jäsenvaltion kanssa erikseen, jotta voidaan ottaa huomioon tietoturvavaatimukset, laitteiden fyysinen sijainti ja asennusolosuhteet sekä verkkopalvelun tarjoajan palvelut. Tämä tarkoittaa, että fyysinen s-TESTA-yhteys voi sisältää useita VPN-kanavia myös muiden järjestelmien kuten viisumitietojärjestelmän (VIS) ja Eurodacin tarpeita silmällä pitäen.

— kansallinen keskusliittymä, jäljempänä 'CNI', eli sovellus, joka varmistaa pääsyn SIS II -tietokantaan (CS-SIS). Kullakin jäsenvaltiolla on oma looginen liitäntäpiste kansalliseen keskusliittymään keskuspalomuurin kautta.

CS-SIS:n ja NI-SIS:ien välinen viestintäinfrastruktuuri muodostuu seuraavista osista:

— s-TESTA-verkko (Secure Trans-European Services for Telematics between Administrations), jäljempänä 's-TESTA', joka tarjoaa suojatun virtuaalisen erillisverkon SIS II -tietoja ja SIRENE-tietojenvaihtoa varten.

3. **Maantieteellinen kattavuus**

Viestintäinfrastruktuurin tulee kattaa kaikki järjestelmän toimintaan osallistuvat valtiot, ja sen on pystyttävä tarjoamaan niille kaikki vaaditut palvelut:

Kaikki EU:n jäsenvaltiot (Alankomaat, Belgia, Espanja, Irlanti, Italia, Itävalta, Kreikka, Kypros, Latvia, Liettua, Luxemburg, Malta, Portugali, Puola, Ranska, Ruotsi, Saksa, Slovakia, Slovenia, Suomi, Tanska, Tšekki, Unkari, Viro ja Yhdistynyt kuningaskunta) sekä Norja, Islanti ja Sveitsi.

Lisäksi on varauduttava Romanian ja Bulgarian liittymiseen Schengenin tietojärjestelmään.

Viestintäinfrastruktuuriin on myös voitava liittää SIS II -keskusjärjestelmään mahdollisesti myöhemmin liittyvät maat tai yksiköt (esim. Europol, Eurojust).

4. **Verkkopalvelut**

Aina kun mainitaan jokin protokolla tai arkkitehtuuri, myös vastaavat uudemmat teknologiat, protokollat ja arkkitehtuurit ovat hyväksyttäviä.

4.1 *Verkon toimintamalli*

SIS II:n arkkitehtuuri perustuu keskitettyihin palveluihin, joita voidaan käyttää eri jäsenvaltioissa. Järjestelmän häiriönsietokyvyn turvaamiseksi keskitetyt palvelut on kopioitu kahteen eri paikkaan siten, että pääjärjestelmä (CS-SIS) ja keskusyksikkö (CU) sijaitsevat Strasbourgissa Ranskassa ja niiden varmuusjärjestelmät St. Johann im Pongaussa Itävallassa.

Sekä pää- että varmuuskeskusyksikköön on voitava luoda yhteys kaikista tietojärjestelmään kuuluvista jäsenvaltioista. Järjestelmään osallistuvilla valtioilla voi olla useampia verkkoliitäntäpisteitä, yksi kansallinen paikallisliittymä ja sen varmuusjärjestelmä, joiden kautta niiden kansallinen järjestelmä on liitetty keskusjärjestelmään.

Sen lisäksi, että viestintäinfrastruktuurin avulla luodaan järjestelmän toiminnan kannalta keskeinen yhteys kustakin jäsenvaltiosta keskusjärjestelmään, sen avulla on myös voitava välittää lisätietoja kahdenvälisesti eri jäsenvaltioiden SIRENE-toimistojen välillä.

4.2 *Pää- ja varmuusjärjestelmän yhteystyyppi*

Pääjärjestelmän ja varmuusjärjestelmän välisen yhteystyypin on oltava SDH-ring tai vastaava, eli siinä on voitava käyttää myös uusia arkkitehtuureja ja teknologioita. SDH-infrastruktuurin avulla on myös tarkoitus laajentaa kummankin keskusyksikön paikallisverkkoja, jotta voidaan luoda saumattomasti toimiva yhtenäinen lähiverkko (LAN). Tämän lähiverkon avulla toteutetaan keskusyksikön ja sen varmuusjärjestelmän jatkuva synkronointi.

4.3 *Kaistanleveys*

Olennainen viestintäinfrastruktuuria koskeva vaatimus liittyy kaistanleveyteen, jonka se pystyy tarjoamaan toisiinsa liitetyille asemille (site), ja sen kyky tukea tätä kaistanleveyttä runkoverkossaan.

Kansallista paikallisliittymää (LNI) ja sen mahdollista varmuusjärjestelmää (BLNI) varten tarvittava kaistanleveys vaihtelee jäsenvaltiosta toiseen sen mukaan, käyttävätkö ne kansallisia kopioita, tietojen hakua keskustietojärjestelmästä ja biometristen tietojen vaihtoa.

Sillä, minkä verran kaistanleveyttä viestintäinfrastruktuurista annetaan eri valtioille, ei ole merkitystä, kunhan kaistanleveys riittää täyttämään kunkin jäsenvaltion vähimmäistarpeet.

Kukin edellä mainituista erilaisista asemista voi siirtää suuria määriä tietoja (aakkosnumeerisia ja biometrisiä tietoja sekä kokonaisia asiakirjoja) kumpaankin suuntaan. Tämän vuoksi viestintäinfrastruktuurin on taattava kullekin yhteydelle riittävän suuri vähimmäissiirtonopeus kumpaankin suuntaan tapahtuvia siirtoja varten.

Viestintäinfrastruktuurin on voitava tarjota yhteyksiä, joiden nopeus on vähintään 2 Mb/s ja jopa 155 Mb/s tai enemmän. Verkon on taattava kullekin yhteydelle riittävän suuri vähimmäissiirtonopeus kumpaankin suuntaan tapahtuvia siirtoja varten ja sen on pystyttävä tarjoamaan tuki verkkoliitäntäpisteiden kokonaiskaistanleveydelle.

4.4 *Palveluluokat*

SIS II:n keskustietojärjestelmässä on myös jatkossa mahdollista priorisoida tiettyjä hakuja/kuulutuksia. Tämän vuoksi myös viestintäinfrastruktuurissa on voitava priorisoida tietoliikennettä.

SIS II:n keskustietojärjestelmän oletetaan asettavan verkon priorisointiparametrit kaikkia niitä tiedonsiirtopaketteja varten, jotka sitä vaativat. Tätä varten käytetään WFQ-jonotusmenetelmää (Weighted Fair Queuing). Tämä edellyttää, että viestintäinfrastruktuuri pystyy omaksumaan lähettävän lähiverkon tietopaketille antaman priorisointiluokituksen ja käsittelemään paketteja runkoverkossaan sen mukaisesti. Lisäksi viestintäinfrastruktuurin on pystyttävä toimittamaan alkuperäiset paketit määränpäähän niin, että niissä on edelleen lähettävän lähiverkon antama priorisointiluokitus.

4.5 *Tuetut protokollat*

SIS II:n keskusyksikössä käytetään useita verkkoprotokollia. Siksi viestintäinfrastruktuurin on tuettava useita erilaisia verkkoprotokollia. Tällaisia vakiokäytössä olevia protokollia ovat HTTP, FTP, NTP, SMTP, SNMP ja DNS.

Vakioprotokollien lisäksi viestintäinfrastruktuurin on pystyttävä käsittelemään myös erilaisia tunnelointiprotokollia, tallennusverkon (SAN) replikointiprotokollia sekä BEA WebLogicin omia Java-to-Java-yhteysprotokollia. Tunnelointiprotokollia, mm. IPsec-protokollaa, käytetään suojattujen pakettien siirtämiseen lähettäjältä vastaanottajalle.

4.6 *Tekniset eritelmät*

4.6.1 IP-osoitejärjestelmä

Viestintäinfrastruktuurin tulee sisältää joukko varattuja IP-osoitteita, joita voidaan käyttää ainoastaan tämän verkon sisällä. SIS II:ssa käytetään vain tiettyä osaa näistä varatuista IP-osoitteista, eikä niitä käytetä missään muualla.

4.6.2 Ipv6-osoitteiden käyttö

Voidaan olettaa, että jäsenvaltioiden paikallisverkoissa käytetään TCP/IP-protokollaa. Jotkut asemat käyttävät kuitenkin 4-versiota ja toiset 6-versiota. Verkkoliitäntäpisteiden on voitava toimia yhdyskäytävänä sekä SIS II:n keskusjärjestelmän ja N.SIS II:n käyttämistä verkkoprotokollista riippumattomasti.

4.6.3 Staattinen reitityksenvalinta

Keskus- ja varmuusjärjestelmä voivat käyttää jäsenvaltioiden kanssa käytävässä viestinnässä samaa IP-osoitetta. Siksi viestintäinfrastruktuurin olisi voitava tukea staattista reitityksenvalintaa.

4.6.4 Kaistanleveyden kapasiteetti

Jos keskus- tai varmuusjärjestelmän käyttämä osuus yhteydestä alle 90 prosenttia, yksittäisen jäsenvaltion on voitava tukea jatkuvasti 100 prosenttia sille myönnetystä kaistanleveydestä.

4.6.5 Muut vaatimukset

CS-SIS:n toimintavaatimusten täyttämiseksi viestintäinfrastruktuurin on täytettävä ainakin seuraavat tekniset vaatimukset:

Tiedonsiirtojen kauttakulkuviive saa olla (myös ruuhka-aikoina) enintään 150 ms 95 prosentilla paketeista ja alle 200 ms 100 prosentilla paketeista.

Tietopakettien katoamisen todennäköisyys saa olla (myös ruuhka-aikoina) enintään 10^{-4} 95 prosentilla paketeista ja alle 10^{-3} 100 prosentilla paketeista.

Nämä vaatimukset koskevat kutakin liitäntäpistettä erikseen.

Keskus- ja varmuusjärjestelmän välisessä yhteydessä kiertokulkuaika saa olla enintään 60 ms.

4.7 *Häiriönkestävyys*

CS-SIS:n suunnittelussa on pyritty mahdollisimman korkeaan käytettävyyteen. Osien rikkoutumisesta aiheutuvat toimintahäiriöt on pyritty estämään siten, että koko laitteisto on olemassa kahtena kappaleena.

Myös viestintäinfrastruktuurin osien on voitava kestää osien vikaantumisesta aiheutuvat häiriöt. Viestintäinfrastruktuurin osalta tämä tarkoittaa sitä, että seuraavien osien on oltava vikasietoisia:

— runkoverkko

— reitittimet

— liitäntäpisteet

— tilaajayhteydet (fyysisesti redundatti kaapelointi mukaan luettuna)

— tietoturvavälineet (salauslaitteet, palomuurit jne.)

— kaikki yleisluonteiset palvelut (DNS, NTP jne.)

— LNI/BLNI

Kaikkien verkkolaitteiden korjausmekanismien tulisi käynnistyä ilman manuaalisia toimenpiteitä.

5. **Seuranta**

Seurannan helpottamiseksi viestintäinfrastruktuurin seurantavälineet on voitava integroida sen organisaation seurantavälineisiin, joka vastaa SIS II:n keskusyksikön operatiivisesta hallinnoinnista.

6. **Yleisluonteiset palvelut**

Erityisten verkko- ja tietoturvapalvelujen ohella viestintäinfrastruktuurin on kyettävä tarjoamaan myös yleisluonteisia palveluja.

Käyttövarmuuden turvaamiseksi erityispalvelut on toteutettava kummassakin keskusyksikössä.

Viestintäinfrastruktuurin tulee sisältää seuraavat valinnaiset yleisluonteiset palvelut:

Palvelu	Lisätiedot
DNS	Tätä nykyä käytössä oleva mekanismi, jonka avulla vikatilanteessa siirrytään keskusjärjestelmästä varmuusjärjestelmään, jos verkon toimintahäiriö johtuu IP-osoitteen vaihtamisesta yleisellä nimipalvelimella (DNS).
Sähköpostiyhteys	Voi olla kätevää käyttää yleistä sähköpostiyhteyttä, sillä sen avulla eri jäsenvaltioiden sähköpostiasetukset voidaan yhdenmukaistaa. Lisäetuna on se, että näin tähän ei tarvitse käyttää keskus- tai varmuusjärjestelmän verkkokapasiteettia, kuten oman erillisen palvelimen yhteydessä. Yleisen sähköpostiyhteyden kautta välitettävien viestien on joka tapauksessa täytettävä niille asetettavat turvallisuusvaatimukset.
NTP	Tämän palvelun avulla synkronoidaan verkkolaitteiden kellot.

7. **Käytettävyys**

SIS II:n keskusjärjestelmän sekä kansallisten paikallisliittymien ja niiden varmuusjärjestelmien on voitava taata 99,99 prosentin käytettävyys 28 päivän ominaisperiodin ajan ilman että verkon käytettävyyttä lasketaan mukaan.

Viestintäinfrastruktuurin käytettävyyden on oltava 99,99 prosenttia.

8. **Tietoturvapalvelut**

8.1 *Verkon salaus*

SIS II:n keskusjärjestelmä ei salli korkean tai erittäin korkean turvaluokituksen omaavan datan siirtämistä lähiverkon ulkopuolelle ilman salausta. On varmistettava, että verkkopalvelujen tarjoaja ei pääse käsiksi SIS II:n operatiivisiin tietoihin eikä niihin liittyvään SIRENE-tietojenvaihtoon.

Jotta voidaan säilyttää korkea tietoturvan taso, viestintäinfrastruktuurin on mahdollistettava varmenteiden/avainten hallinta. Salauslaitteita on voitava hallinnoida ja valvoa myös etäältä. Salausalgoritmien on täytettävä ainakin seuraavat vaatimukset:

— Symmetriset salausalgoritmit:

• 3DES (128 bittiä) tai parempi

• salausavain on luotava satunnaisluvun avulla, niin että avainta ei ole mahdollista lyhentää hyökkäyksen aikana

• salausavaimet tai tiedot, joiden avulla avaimet voidaan johtaa, on aina suojattava kun ne on tallennettu.

— Epäsymmetriset salausalgoritmit:

• RSA (1 024-bittinen moduuli) tai parempi

• salausavain on luotava satunnaisluvun avulla, niin että avainta ei ole mahdollista lyhentää hyökkäyksen aikana

Salauksessa käytetään ESP-protokollaa (Encapsulated Security Payload, RFC2406) tunneloituna. Payload ja alkuperäiset IP-otsikkotiedot salataan.

Tilapäisten avainten vaihdossa käytetään IKE-protokollaa (Internet Key Exchange).

IKE-avainten voimassaoloaika on enintään yksi päivä.

Tilapäisten avainten voimassaoloaika on enintään yksi tunti.

8.2 *Muut tietoturvaominaisuudet*

Viestintäinfrastruktuurin on suojattava paitsi SIS II:n liityntäpisteet myös valinnaiset yleisluonteiset palvelut. Näiden palvelujen tulee täyttää samat suojatoimet kuin keskusjärjestelmän (CS-SIS). Kaikkien yleisluonteisten palvelujen suojana on näin ollen oltava ainakin palomuuri, viruksentorjuntaohjelma sekä tunkeilijan havaitsemisjärjestelmä. Lisäksi yleisluonteisten palvelujen tuottamisessa käytettävien laitteiden ja niiden suojatoimien on oltava jatkuvan tietoturvavalvonnan alaisia (sisäänkirjaus ja seuranta).

Korkean tietoturvatason säilyttämiseksi SIS II:n keskusjärjestelmän operatiivisesta hallinnoinnista vastaavan organisaation on oltava tietoinen kaikista viestintäinfrastruktuuriin liittyvistä tietoturvaloukkauksista. Tämän vuoksi kaikista viestintäinfrastruktuuriin kohdistuvista tietoturvaloukkauksista on voitava ilmoittaa viipymättä SIS II:n keskusjärjestelmän operatiivisesta hallinnoinnista vastaavalle organisaatiolle. Kaikista tietoturvaloukkauksista on laadittava raportti säännöllisesti, esimerkiksi kuukausittain, ja tapauskohtaisesti.

9. **Käyttötuki ja tukitoiminnot**

Viestintäinfrastruktuurin toimittajan on perustettava myös käyttötuki, joka toimii yhteistyössä SIS II:n keskusjärjestelmän operatiivisesta hallinnoinnista vastaavan organisaation kanssa.

10. **Vuorovaikutus muiden järjestelmien kanssa**

Viestintäinfrastruktuurin on varmistettava, ettei tietoja pääse hyväksyttyjen viestintäkanavien ulkopuolelle. Teknisen toteutuksen kannalta tämä edellyttää, että:

— Kaikki luvaton ja/tai valvomaton pääsy muihin verkkoihin on ankarasti kielletty. Tämä koskee myös yhdysliikennettä Internetiin.

— Tietoja ei saa vuotaa verkon muihin järjestelmiin; esimerkiksi eri IP VPN -verkkojen yhteenliittäminen ei ole sallittua.

Edellä mainittujen teknisten rajoitusten ohella tämä vaatimus vaikuttaa myös viestintäinfrastruktuurin käyttötukeen. Käyttötuki ei saa paljastaa mitään SIS II:n keskusjärjestelmää koskevia tietoja muille kuin SIS II:n keskusjärjestelmän operatiivisesta hallinnoinnista vastaavalle organisaatiolle.