II

(Besluiten op grond van het EG- en het Euratom-Verdrag waarvan publicatie niet verplicht is)

BESLUITEN/BESCHIKKINGEN

COMMISSIE

BESCHIKKING VAN DE COMMISSIE

van 16 maart 2007

tot vaststelling van de netwerkvereisten voor het Schengeninformatiesysteem II (eerste pijler)

(Kennisgeving geschied onder nummer C(2007) 845)

(Slechts de teksten in de Bulgaarse, de Duitse, de Estse, de Finse, de Franse, de Griekse, de Hongaarse, de Italiaanse, de Letse, de Litouwse, de Maltese, de Nederlandse, de Poolse, de Portugese, de Roemeense, de Sloveense, de Slowaakse, de Spaanse, de Tsjechische en de Zweedse taal zijn authentiek)

(2007/170/EG)

DE COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap,

Gelet op Verordening (EG) nr. 2424/2001 van de Raad van 6 december 2001 betreffende de ontwikkeling van een Schengeninformatiesysteem van de tweede generatie (SIS II) [1], en met name op artikel 4, onder a),

Overwegende hetgeen volgt:

(1) Met het oog op de ontwikkeling van SIS II dienen technische specificaties voor het communicatienetwerk en de componenten daarvan, alsmede de specifieke netwerkvereisten, te worden vastgesteld.

(2) Passende regelingen voor de Commissie en de lidstaten dienen te worden vastgesteld inzake met name de onderdelen van de uniforme nationale interfaces in de lidstaten.

(3) Deze beschikking doet geen afbreuk aan de toekomstige aanneming van andere besluiten van de Commissie betreffende de ontwikkeling van SIS II, met name wat betreft de ontwikkeling van de beveiligingseisen.

(4) De ontwikkeling van SIS II is geregeld bij zowel Verordening (EG) nr. 2424/2001 als Besluit 2001/886/JBZ van de Raad [2]. Met het oog op de eenheid van het implementatieproces voor de ontwikkeling van SIS II dienen de bepalingen van dit besluit overeen te stemmen met de bepalingen van het besluit van de Commissie tot vaststelling van de netwerkvereisten voor het Schengeninformatiesysteem II dat uit hoofde van Besluit 2001/886/JBZ wordt vastgesteld.

(5) Overeenkomstig Besluit 2000/365/EG van de Raad van 29 mei 2000 betreffende het verzoek van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland deel te mogen nemen aan enkele van de bepalingen van het Schengenacquis [3] heeft het Verenigd Koninkrijk niet deelgenomen aan de aanneming van Verordening (EG) nr. 2424/2001 en is die verordening niet bindend voor, noch van toepassing op deze lidstaat, aangezien die verordening een ontwikkeling inhoudt van de bepalingen van het Schengenacquis. Deze beschikking van de Commissie is derhalve niet tot het Verenigd Koninkrijk gericht.

(6) Overeenkomstig Besluit 2002/192/EG van de Raad van 28 februari 2002 betreffende het verzoek van Ierland deel te mogen nemen aan bepalingen van het Schengenacquis [4] heeft Ierland niet deelgenomen aan de aanneming van Verordening (EG) nr. 2424/2001 en is die verordening niet bindend voor, noch van toepassing op deze lidstaat, aangezien die verordening een ontwikkeling inhoudt van de bepalingen van het Schengenacquis. Deze beschikking van de Commissie is derhalve niet tot Ierland gericht.

[1] PB L 328 van 13.12.2001, blz. 4. Verordening gewijzigd bij Verordening (EG) nr. 1988/2006 (PB L 411 van 30.12.2006, blz. 1).
[2] PB L 328 van 13.12.2001, blz. 1.
[3] PB L 131 van 1.6.2000, blz. 43. Besluit gewijzigd bij Besluit 2004/926/EG (PB L 395 van 31.12.2004, blz. 70).
[4] PB L 64 van 7.3.2002, blz. 20.

(7) Overeenkomstig artikel 5 van het Protocol betreffende de positie van Denemarken, dat aan het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap is gehecht, heeft Denemarken besloten Verordening (EG) nr. 2424/2001 van de Raad in het Deense recht ten uitvoer te leggen. Verordening (EG) nr. 2424/2001 is derhalve volgens internationaal recht bindend voor Denemarken.

(8) Wat IJsland en Noorwegen betreft, houden Verordening (EG) nr. 2424/2001 en Besluit 2001/886/JBZ een ontwikkeling in van bepalingen van het Schengenacquis, zoals bedoeld in de Overeenkomst tussen de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen inzake de wijze waarop IJsland en Noorwegen worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis [1], die vallen onder artikel 1, punt B, van Besluit 1999/437/EG van de Raad van 17 mei 1999 inzake bepaalde toepassingsbepalingen van de door de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen gesloten overeenkomst inzake de wijze waarop deze twee staten worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis [2].

(9) Wat Zwitserland betreft, houden Verordening (EG) nr. 2424/2001 en Besluit 2001/886/JBZ een ontwikkeling in van de bepalingen van het Schengenacquis in de zin van de Overeenkomst die is ondertekend door de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis, die vallen onder het gebied bedoeld in artikel 4, lid 1, van Besluit 2004/860/EG van de Raad betreffende de ondertekening, namens de Europese Gemeenschap, en de voorlopige toepassing van enkele bepalingen van die overeenkomst.

(10) Dit besluit is een rechtsbesluit dat voortbouwt op het Schengenacquis of op een andere wijze daaraan is gerelateerd, zoals bedoeld in artikel 3, lid 1, van de Toetredingsakte.

(11) De maatregelen waarin deze beschikking voorziet, zijn in overeenstemming met het advies van het bij artikel 5, lid 1, van Verordening (EG) nr. 2424/2001 ingestelde comité,

HEEFT DE VOLGENDE BESCHIKKING GEGEVEN:

Artikel 1

De technische specificaties met betrekking tot de opzet van de fysieke architectuur van de communicatie-infrastructuur van SIS II zijn die welke in de bijlage zijn opgenomen.

Artikel 2

Deze beschikking is gericht tot het Koninkrijk België, de Republiek Bulgarije, de Tsjechische Republiek, de Bondsrepubliek Duitsland, de Republiek Estland, de Helleense Republiek, het Koninkrijk Spanje, de Franse Republiek, de Italiaanse Republiek, de Republiek Cyprus, de Republiek Letland, de Republiek Litouwen, het Groothertogdom Luxemburg, de Republiek Hongarije, de Republiek Malta, het Koninkrijk der Nederlanden, de Republiek Oostenrijk, de Republiek Polen, de Portugese Republiek, Roemenië, de Republiek Slovenië, de Slowaakse Republiek, de Republiek Finland en het Koninkrijk Zweden.

Gedaan te Brussel, 16 maart 2007.

Voor de Commissie
Franco FRATTINI
Vicevoorzitter

[1] PB L 176 van 10.7.1999, blz. 36.
[2] PB L 176 van 10.7.1999, blz. 31.

BIJLAGE

INHOUD

1. **Inleiding**

In dit document worden de opzet van het communicatienetwerk, de verschillende componenten ervan en de specifieke netwerkvereisten beschreven.

1.1. *Acroniemen en afkortingen*

In dit document worden de onderstaande acroniemen en afkortingen gebruikt.

Acroniemen en afkortingen	Betekenis
BLNI	Back-up van de lokale nationale interface
CEP	Centraal eindpunt
CNI	Centrale nationale interface
CS	Centraal systeem
CS-SIS	Technisch ondersteunende functie die de SIS II-databank bevat
DNS	Domeinnaamserver
FCIP	Fibre Channel over IP
FTP	File Transport Protocol
HTTP	Hyper Text Transfer Protocol
IP	Internetprotocol
LAN	Local Area Network
LNI	Lokale nationale interface
Mbps	Megabit per seconde
MDC	Hoofdcontractant voor de ontwikkeling
N.SIS II	Nationaal deel van SIS II in elke lidstaat
NI-SIS	Uniforme nationale interface
NTP	Network Time Protocol
SAN	Storage Area Network
SDH	Synchronous Digital Hierarchy
SIS II	Schengeninformatiesysteem van de tweede generatie
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
s-TESTA	Secure Trans-European Services for Telematics between Administrations — beveiligde trans-Europese diensten voor telematica tussen overheidsdiensten. Dit is een onderdeel van het IDABC-programma (interoperabele levering van pan-Europese e-overheidsdiensten aan overheidsdiensten, ondernemingen en burgers. Besluit 2004/387/EG van het Europees Parlement en de Raad van 21 april 2004).
TCP	Transmission Control Protocol
VIS	Visuminformatiesysteem
VPN	Virtual Private Network
WAN	Wide Area Network

2. **Algemeen overzicht**

SIS II bestaat uit:

— het centrale systeem (hierna het „centrale SIS II" genoemd), bestaande uit:

  • een technisch ondersteunende functie (hierna „CS-SIS" genoemd) die de SIS II-gegevensbank bevat. CS-SIS zorgt voor technisch toezicht en beheer. Een back-up van CS-SIS kan alle functionaliteit van het normale CS-SIS overnemen, mocht dat systeem uitvallen;

  • een uniforme nationale interface (hierna „NI-SIS" genoemd);

— een nationaal deel (hierna „N.SIS II" genoemd) in elk van de lidstaten, bestaande uit de nationale datasystemen die in verbinding staan met het centrale SIS II. Een N.SIS II kan een gegevensbestand bevatten (hierna „nationale kopie" genoemd) dat een volledige of gedeeltelijke kopie bevat van de SIS II-gegevensbank;

— een communicatie-infrastructuur tussen CS-SIS en NI-SIS (hierna „communicatie-infrastructuur" genoemd), waarmee een versleuteld virtueel netwerk tot stand wordt gebracht dat specifiek bestemd is voor SIS II-gegevens en voor de uitwisseling van gegevens tussen de Sirenebureaus.

NI-SIS bestaat uit:

— één lokale nationale interface (hierna „LNI" genoemd) in iedere lidstaat, die de fysieke verbinding vormt tussen de lidstaat en het beveiligde communicatienetwerk en waarin de versleutelingsapparatuur voor het SIS II-verkeer en het Sireneverkeer is opgenomen. De LNI bevindt zich in gebouwen van de lidstaat.

— een optionele back-up van de lokale nationale interface (hierna „BLNI" genoemd) met exact dezelfde inhoud en functie als de LNI.

De LNI en de BLNI worden uitsluitend gebruikt door het SIS II-systeem en voor het Sireneverkeer. De specifieke configuratie van de LNI en de BLNI wordt met elke afzonderlijke lidstaat overeengekomen, afhankelijk van de beveiligingseisen, de fysieke locatie en de specifieke omstandigheden van de installatie. Dit geldt ook voor de verlening van diensten door de netwerkprovider, dat wil zeggen dat over de fysieke s-TESTA-verbinding verschillende VPN-tunnels kunnen worden opgezet voor andere systemen, bijvoorbeeld VIS en Eurodac.

— een centrale nationale interface (hierna „CNI" genoemd): een applicatie voor de beveiliging van de toegang tot CS-SIS. Elke lidstaat heeft zijn eigen logische toegangspunten tot de CNI, via een centrale firewall.

De communicatie-infrastructuur tussen CS-SIS en NI-SIS bestaat uit:

— het netwerk voor beveiligde trans-Europese diensten voor telematica tussen overheidsdiensten (hierna „s-TESTA" genoemd), dat een versleuteld Virtual Private Network biedt dat specifiek bestemd is voor SIS II-gegevens en voor Sireneverkeer.

3. **Geografisch toepassingsgebied**

De communicatie-infrastructuur moet alle lidstaten bereiken en aan alle lidstaten de vereiste diensten kunnen verlenen:

Dit geldt voor de lidstaten (België, Frankrijk, Duitsland, Luxemburg, Nederland, Italië, Portugal, Spanje, Griekenland, Oostenrijk, Denemarken, Finland, Zweden, Cyprus, Tsjechië, Estland, Hongarije, Letland, Litouwen, Malta, Polen, Slowakije, Slovenië, het Verenigd Koninkrijk en Ierland) en voor Noorwegen, IJsland en Zwitserland.

Bovendien moet worden voorzien in uitbreiding van de dekking tot de toetredende landen Bulgarije en Roemenië.

Tot slot moet de communicatie-infrastructuur kunnen worden uitgebreid tot elk ander land dat of elke andere entiteit die op het centrale SIS II wordt aangesloten (bijvoorbeeld Europol, Eurojust).

4. **Netwerkdiensten**

Wanneer een bepaald protocol of een bepaalde architectuur wordt genoemd, zijn gelijkwaardige toekomstige technologieën, protocollen en architecturen ook aanvaardbaar.

4.1. *Opzet van het netwerk*

De SIS II-architectuur maakt gebruik van gecentraliseerde diensten die vanuit de verschillende lidstaten toegankelijk zijn. Omwille van de betrouwbaarheid worden deze gecentraliseerde diensten in tweevoud uitgevoerd en op twee verschillende locaties ondergebracht, namelijk in Straatsburg in Frankrijk (CS-SIS en centrale eenheid of CU) en St. Johann im Pongau in Oostenrijk (back-up van CS-SIS en back-up van de centrale eenheid of BCU).

De centrale eenheid en de back-up van de centrale eenheid moeten vanuit alle lidstaten toegankelijk zijn. De deelnemende landen kunnen via verschillende toegangspunten tot het netwerk, een LNI en een BLNI, een verbinding met de centrale diensten opzetten.

Naast de hoofdverbinding met de centrale diensten moet de communicatie-infrastructuur ook aanvullende bilaterale informatie-uitwisseling tussen de Sirenebureaus van de lidstaten ondersteunen.

4.2. *Type verbinding tussen CS-SIS en back-up van CS-SIS*

Het vereiste verbindingstype voor de connectiviteit tussen CS-SIS en de back-up van CS-SIS is een SDH-ring of een gelijkwaardig verbindingstype, dat wil zeggen dat nieuwe toekomstige architecturen en technologieën ook moeten kunnen worden toegepast. De SDH-infrastructuur wordt gebruikt om de lokale netwerken van beide centrale eenheden uit te breiden en zo één naadloos LAN te creëren. Dit LAN wordt dan gebruikt voor de continue synchronisatie tussen CU en BCU.

4.3. *Bandbreedte*

Een essentiële eis die aan de communicatie-infrastructuur wordt gesteld, betreft de bandbreedte die aan de verschillende verbonden locaties kan worden toegekend en het vermogen om deze bandbreedte in het backbone-netwerk te ondersteunen.

De voor de LNI en de optionele BLNI benodigde bandbreedte zal voor elke lidstaat verschillend zijn, afhankelijk van de keuze voor het gebruik van een nationale kopie, centraal zoeken en uitwisseling van biometrische gegevens.

De precieze bandbreedte die door de communicatie-infrastructuur wordt aangeboden, is niet van belang, zolang aan de minimale behoeften van elke lidstaat wordt voldaan.

Door elk van de genoemde soorten locaties worden in beide richtingen grote hoeveelheden gegevens verzonden (alfanumerieke en biometrische gegevens en volledige documenten). De communicatie-infrastructuur moet voor elke verbinding daarom een toereikende minimale gegarandeerde upload- en downloadsnelheid bieden.

De communicatie-infrastructuur moet bandbreedten kunnen bieden van 2 Mbps tot 155 Mbps of meer. Het netwerk moet voor elke verbinding een toereikende minimale gegarandeerde upload- en downloadsnelheid bieden, en zodanig zijn opgezet dat de totale bandbreedte van alle toegangspunten tot het netwerk kan worden ondersteund.

4.4. *Serviceklasse*

Het centrale SIS II biedt de mogelijkheid om aan opzoekingen/signaleringen prioriteit toe te kennen. Een afgeleide eis is dat de communicatie-infrastructuur ook de mogelijkheid van prioritering van verkeer moet ondersteunen.

De parameters die het netwerk voor de prioritering toepast, worden geacht te worden vastgesteld door het centrale SIS II voor alle pakketten waarvoor dat nodig is. Daarbij wordt gebruik gemaakt van Weighted Fair Queuing. Dit betekent dat de communicatie-infrastructuur de prioritering die het LAN van herkomst aan de gegevenspakketten heeft toegekend, moet kunnen overnemen en de pakketten binnen haar eigen backbone-netwerk dienovereenkomstig moet afhandelen. Bovendien moet de communicatie-infrastructuur de oorspronkelijke pakketten bij de bestemmingslocatie afleveren met dezelfde prioritering als door het LAN van herkomst is toegekend.

4.5. *Ondersteunde protocollen*

Het centrale SIS II maakt gebruik van een aantal netwerkcommunicatieprotocollen. De communicatie-infrastructuur moet een groot aantal netwerkcommunicatieprotocollen ondersteunen. De standaard te ondersteunen protocollen zijn HTTP, FTP, NTP, SMTP, SNMP en DNS.

Naast de standaardprotocollen moet de communicatie-infrastructuur ook kunnen omgaan met verschillende tunnelprotocollen, SAN-replicatieprotocollen en de merkgebonden Java-to-Java-verbindingsprotocollen van BEA WebLogic. De tunnelprotocollen, bijvoorbeeld IPsec in tunnelmodus, worden gebruikt voor het transport van versleutelde gegevens naar hun bestemming.

4.6. *Technische specificaties*

4.6.1. IP-adressering

De communicatie-infrastructuur moet beschikken over een reeks gereserveerde IP-adressen die uitsluitend binnen dat netwerk worden gebruikt. Binnen de reeks gereserveerde IP-adressen gebruikt het centrale SIS II een specifiek aantal IP-adressen die nergens anders worden gebruikt.

4.6.2. Ondersteuning voor IPv6

Er mag worden verondersteld dat de lokale netwerken van de lidstaten gebruik maken van het TCP/IP-protocol. Sommige locaties zullen echter versie 4 gebruiken, andere versie 6. De toegangspunten tot het netwerk moeten als gateway kunnen functioneren en onafhankelijk kunnen werken van de netwerkprotocollen die in het centrale SIS II en het N.SIS II worden gebruikt.

4.6.3. Static Route Injection

De CU en de BCU kunnen voor de communicatie met de lidstaten hetzelfde IP-adres gebruiken. De communicatie-infrastructuur moet daarom static route injection ondersteunen.

4.6.4. Sustained Flow Rate

Zolang de verbinding met de CU of de BCU voor minder dan 90 % wordt belast, moet een gegeven lidstaat continu 100 % van de voor die lidstaat gespecificeerde bandbreedte kunnen aanhouden.

4.6.5. Andere specificaties

Om CS-SIS te kunnen ondersteunen, moet de communicatie-infrastructuur ten minste aan een aantal minimale technische specificaties voldoen:

De doorvoertijd mag (ook in de piekuren) voor 95 % van de pakketten niet meer dan 150 ms bedragen en moet voor 100 % van de pakketten minder dan 200 ms bedragen.

De kans dat pakketverlies optreedt mag (ook in de piekuren) voor 95 % van de pakketten niet meer dan 10^{-4} bedragen en moet voor 100 % van de pakketten minder dan 10^{-3} bedragen.

Bovengenoemde specificaties moeten gelden voor elk toegangspunt afzonderlijk.

Voor de verbinding tussen de CU en de BCU mag de transmissievertraging heen en terug niet meer dan 60 ms bedragen.

4.7. *Herstellingsvermogen*

Bij het ontwerpen van CS-SIS was de eis dat het systeem door een hoge graad van beschikbaarheid wordt gekenmerkt. Alle apparatuur is daarom dubbel uitgevoerd, zodat het systeem zich kan herstellen wanneer er een onderdeel uitvalt.

Ook de onderdelen van de communicatie-infrastructuur moeten bestand zijn tegen uitval van een onderdeel. Voor de communicatie-infrastructuur betekent dit dat de volgende onderdelen tegen uitval bestand moeten zijn:

— backbone-netwerk;

— routingapparatuur;

— aanwezigheidspunten (points of presence);

— lokale aansluitverbindingen (met inbegrip van fysiek redundante bekabeling);

— beveiligingsapparatuur (versleuteling, firewalls, enz.);

— alle generieke diensten (DNS, NTP, enz.);

— LNI/BLNI

De failover-mechanismen moeten voor alle netwerkapparatuur automatisch in werking treden, zonder enige vorm van handmatige interventie.

5. **Monitoring**

Om de monitoring te vergemakkelijken, moeten de monitoringgereedschappen van de communicatie-infrastructuur kunnen worden geïntegreerd met die van de monitoringfaciliteiten van de organisatie die voor het operationele beheer van het centrale SIS II verantwoordelijk is.

6. **Generieke diensten**

Naast de specifieke netwerk- en beveiligingsdiensten moet de communicatie-infrastructuur ook generieke diensten bieden.

Omwille van de redundantie moeten de specifieke diensten bij beide centrale eenheden worden ondergebracht.

De volgende optionele generieke diensten moeten in de communicatie-infrastructuur aanwezig zijn:

Dienst	Aanvullende informatie
DNS	De failover-procedure voor het overschakelen van CU naar BCU wanneer het netwerk uitvalt, is momenteel gebaseerd op wijziging van het IP-adres in de generieke DNS-server.
Verzending van e-mail	Het gebruik van een generieke e-mail-relay kan nuttig zijn voor het standaardiseren van de e-mailconfiguratie voor de verschillende lidstaten en gebruikt, anders dan een gespecialiseerde server, geen netwerkresources van de CU/BCU. E-mails die via de generieke e-mailrelay worden verzonden, moeten wel voldoen aan de veiligheidseisen.
NTP	Deze dienst kan worden gebruikt voor het synchroniseren van de klok van de netwerkapparatuur.

7. **Beschikbaarheid**

CS-SIS en de LNI en BLNI moeten een beschikbaarheidsgraad van 99,99 % kunnen bieden over een periode van 28 dagen, de netwerkbeschikbaarheid niet in aanmerking genomen.

De beschikbaarheidsgraad van de communicatie-infrastructuur moet 99,99 % zijn.

8. **Beveiligingsdiensten**

8.1. *Netwerkversleuteling*

Het centrale SIS II staat niet toe dat gegevens waarvoor een hoge of zeer hoge beschermingsgraad vereist is, zonder versleuteling buiten het LAN worden gebracht. Er moet worden gegarandeerd dat de netwerkprovider op geen enkele wijze toegang heeft tot de operationele gegevens van SIS II en de daarmee samenhangende Sirene-gegevens.

Om een hoog beveiligingsniveau te kunnen handhaven, moet de communicatie-infrastructuur de mogelijkheid bieden tot beheer van de certificaten/sleutels. Beheer en monitoring van de versleutelingsapparatuur moeten op afstand mogelijk zijn. De versleutelingsalgoritmen moeten ten minste aan de volgende eisen voldoen:

— Symmetrische versleutelingsalgoritmen:

• 3DES (128 bits) of beter

• Bij het genereren van de sleutels moet worden uitgegaan van een toevalswaarde die bij een aanval geen verkleining van de sleutelruimte mogelijk maakt.

• De sleutels, of informatie die kan worden gebruikt om de sleutels te achterhalen, moeten bij de opslag altijd beschermd zijn.

— Asymmetrische versleutelingsalgoritmen:

• RSA (1 024 bit modulus) of beter

• Bij het genereren van de sleutels moet worden uitgegaan van een toevalswaarde die bij een aanval geen verkleining van de sleutelruimte mogelijk maakt.

Er moet gebruik worden gemaakt van het Encapsulated Security Payload-protocol (ESP, RFC2406). Dit protocol wordt gebruikt in tunnelmodus. De payload en de oorspronkelijke IP-header worden versleuteld.

Voor de uitwisseling van sessiesleutels wordt het Internet Key Exchange-protocol (IKE) gebruikt.

De geldigheidsduur van IKE-sleutels moet beperkt zijn tot 1 dag.

De geldigheidsduur van sessiesleutels moet beperkt zijn tot 1 uur.

8.2. *Andere beveiligingskenmerken*

De communicatie-infrastructuur moet niet alleen de toegangpunten tot SIS II beveiligen, maar ook de optionele generieke diensten. Voor deze diensten moeten gelijkwaardige beschermingsmaatregelen gelden als voor CS-SIS. Dat wil zeggen dat alle generieke diensten ten minste met een firewall, antivirus en een inbraakdetectiesysteem moeten worden beschermd. Bovendien moeten de apparatuur voor de generieke diensten en de beschermingsmaatregelen onder voortdurende beveiligingssurveillance staan (logging en follow-up).

Met het oog op de handhaving van een hoog veiligheidsniveau moet de organisatie die voor het operationele beheer van het centrale SIS II verantwoordelijk is, op de hoogte worden gebracht van alle beveiligingsincidenten die zich met betrekking tot de communicatie-infrastructuur voordoen. De communicatie-infrastructuur moet het daarom mogelijk maken dat alle ernstige beveiligingsincidenten onmiddellijk bij de voor het operationele beheer van het centrale SIS II verantwoordelijke organisatie worden gemeld. Van alle beveiligingsincidenten moet regelmatig een overzicht worden gegeven, bijvoorbeeld door maandelijkse rapportage en op ad-hocbasis.

9. **Helpdesk en structuur voor ondersteuning**

De leverancier van de communicatie-infrastructuur moet een helpdeskfaciliteit bieden die samenwerkt met de voor het operationele beheer van het centrale SIS II verantwoordelijke organisatie.

10. **Interactie met andere systemen**

De communicatie-infrastructuur moet garanderen dat informatie binnen de toegewezen communicatiekanalen blijft. Voor de technische implementatie betekent dit dat:

— alle onbevoegde en/of ongecontroleerde toegang tot andere netwerken streng verboden is. Dit heeft ook betrekking op verbinding met het internet.

— het lekken van gegevens naar andere systemen op het netwerk moet onmogelijk zijn; interconnectie van verschillende IP-VPN's is bijvoorbeeld niet toegestaan.

Deze bepaling leidt niet alleen tot de genoemde technische beperkingen, maar heeft ook gevolgen voor de werkwijze van de helpdesk van de communicatie-infrastructuur. De helpdesk mag geen informatie over het centrale SIS II verstrekken aan anderen dan de organisatie die voor het operationele beheer van het centrale SIS II verantwoordelijk is.