II

(Nicht veröffentlichungsbedürftige Rechtsakte, die in Anwendung des EG-Vertrags/Euratom-Vertrags erlassen wurden)

ENTSCHEIDUNGEN UND BESCHLÜSSE

KOMMISSION

ENTSCHEIDUNG DER KOMMISSION

vom 16. März 2007

über die Netzanforderungen für das Schengener Informationssystem der zweiten Generation (erste Säule)

(Bekannt gegeben unter Aktenzeichen K(2007) 845)

(Nur der bulgarische, der deutsche, der estnische, der finnische, der französische, der griechische, der italienische, der lettische, der litauische, der maltesische, der niederländische, der polnische, der portugiesische, der rumänische, der schwedische, der slowakische, der slowenische, der spanische, der tschechische und der ungarische Text sind verbindlich.)

(2007/170/EG)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Verordnung (EG) Nr. 2424/2001 des Rates vom 6. Dezember 2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) [1], insbesondere auf Artikel 4 Buchstabe a,

in Erwägung nachstehender Gründe:

(1) Zur Entwicklung des SIS II müssen technische Spezifikationen für das Kommunikationsnetz, dessen Bestandteile und die besonderen Netzanforderungen festgelegt werden.

(2) Insbesondere zu den Elementen der einheitlichen nationalen Schnittstelle in den Mitgliedstaaten sollten geeignete Vereinbarungen zwischen der Kommission und den Mitgliedstaaten getroffen werden.

(3) Diese Entscheidung greift der späteren Annahme weiterer Kommissionsentscheidungen über die Entwicklung des SIS II, insbesondere zur Ausarbeitung von Sicherheitsanforderungen, nicht vor.

(4) Sowohl die Verordnung (EG) Nr. 2424/2001 als auch der Beschluss 2001/886/JI des Rates [2] regeln die Entwicklung des SIS II. Um ein einheitliches Vorgehen bei der Entwicklung des gesamten SIS II sicherzustellen, sollten die Bestimmungen dieser Entscheidung denen des Kommissionsbeschlusses über die Netzanforderungen für das SIS II entsprechen, der in Anwendung des Beschlusses 2001/886/JI zu erlassen ist.

(5) Gemäß dem Beschluss 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf sie anzuwenden [3], hat sich das Vereinigte Königreich nicht am Erlass der Verordnung (EG) Nr. 2424/2001 beteiligt, die daher weder für das Vereinigte Königreich bindend noch dort anzuwenden ist, da sie den Schengen-Besitzstand weiterentwickelt. Diese Entscheidung der Kommission ist daher nicht an das Vereinigte Königreich gerichtet.

(6) Gemäß dem Beschluss 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland [4] hat sich Irland nicht am Erlass der Verordnung (EG) Nr. 2424/2001 beteiligt, die daher weder für Irland bindend noch dort anzuwenden ist, da sie den Schengen-Besitzstand weiterentwickelt. Diese Entscheidung der Kommission ist daher nicht an Irland gerichtet.

[1] ABl. L 328 vom 13.12.2001, S. 4. Verordnung geändert durch die Verordnung (EG) Nr. 1988/2006 (ABl. L 411 vom 30.12.2006, S. 1).

[2] ABl. L 328 vom 13.12.2001, S. 1.

[3] ABl. L 131 vom 1.6.2000, S. 43. Beschluss geändert durch den Beschluss 2004/926/EG (ABl. L 395 vom 31.12.2004, S. 70).

[4] ABl. L 64 vom 7.3.2002, S. 20.

(7) Dänemark hat gemäß Artikel 5 des dem Vertrag über die Europäische Union und dem Vertrag zur Gründung der Europäischen Gemeinschaft beigefügten Protokolls über die Position Dänemarks beschlossen, die Verordnung (EG) Nr. 2424/2001 in dänisches Recht umzusetzen. Die Verordnung ist daher nach dem Völkerrecht für Dänemark bindend.

(8) Für Island und Norwegen stellen die Verordnung (EG) Nr. 2424/2001 und der Beschluss 2001/886/JI eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung dieser beiden Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands [1] dar, die zu dem Bereich nach Artikel 1 Buchstabe B des Beschlusses 1999/437/EG des Rates vom 17. Mai 1999 zum Erlass bestimmter Durchführungsvorschriften zu dem Übereinkommen zwischen dem Rat der Europäischen Union und der Republik Island und dem Königreich Norwegen über die Assoziierung dieser beiden Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen- Besitzstands [2] gehören.

(9) Für die Schweiz stellen die Verordnung (EG) Nr. 2424/2001 und der Beschluss 2001/886/JI eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar, die zu dem in Artikel 4 Absatz 1 des Beschlusses des Rates über die Unterzeichnung dieses Abkommens im Namen der Europäischen Gemeinschaft und die vorläufige Anwendung einiger Bestimmungen dieses Abkommens genannten Bereich gehören.

(10) Diese Entscheidung ist ein auf dem Schengen-Besitzstand aufbauender oder anderweitig damit zusammenhängender Rechtsakt im Sinne von Artikel 3 Absatz 1 der Beitrittsakte.

(11) Die Maßnahmen dieser Entscheidung stehen im Einklang mit der Stellungnahme des gemäß Artikel 6 Absatz 1 der Verordnung (EG) Nr. 2424/2001 eingesetzten Ausschusses —

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1

Die technischen Spezifikationen für den physischen Aufbau der Kommunikationsinfrastruktur des SIS II werden im Anhang festgelegt.

Artikel 2

Diese Entscheidung ist an das Königreich Belgien, die Republik Bulgarien, die Tschechische Republik, die Bundesrepublik Deutschland, die Republik Estland, die Hellenische Republik, das Königreich Spanien, die Französische Republik, die Italienische Republik, die Republik Zypern, die Republik Lettland, die Republik Litauen, das Großherzogtum Luxemburg, die Republik Ungarn, die Republik Malta, das Königreich der Niederlande, die Republik Österreich, die Republik Polen, die Portugiesische Republik, Rumänien, die Republik Slowenien, die Slowakische Republik, die Republik Finnland und das Königreich Schweden gerichtet.

Brüssel, den 16. März 2007

Für die Kommission
Franco FRATTINI
Vizepräsident

[1] ABl. L 176 vom 10.7.1999, S. 36.
[2] ABl. L 176 vom 10.7.1999, S. 31.

ANHANG

INHALTSVERZEICHNIS

1. Einführung

In diesem Dokument werden der Aufbau des Kommunikationsnetzes, dessen Bestandteile und die besonderen Netzanforderungen beschrieben.

1.1. *Akronyme und Abkürzungen*

Die nachstehende Tabelle enthält die in dem Dokument verwendeten Akronyme und Abkürzungen sowie deren Bedeutung.

Akronyme und Abkürzungen	Bedeutung
BLNI	Backup Local National Interface (lokale nationale Backup-Schnittstelle)
CEP	Central End Point
CNI	Central National Interface (zentrale nationale Schnittstelle)
CS	Central System (zentrales System)
CS-SIS	System zur technischen Unterstützung, das die SIS-II-Datenbank enthält
DNS	Domain Name Server (Domain-Name-Server)
FCIP	Fibre Channel over IP (Glasfaserkanal über IP)
FTP	File Transfer Protocol (Dateiübertragungsprotokoll)
HTTP	Hyper Text Transfer Protocol (Hypertexttransferprotokoll)
IP	Internet Protocol (Internet-Protokoll)
LAN	Local Area Network (lokales Netz)
LNI	Local National Interface (lokale nationale Schnittstelle)
Mbps	Megabits per second (Megabit pro Sekunde)
MDC	Main Developer Contractor
N.SIS II	Nationaler Teil des SIS in jedem Mitgliedstaat
NI-SIS	Einheitliche nationale Schnittstelle
NTP	Network Time Protocol (Netzzeitprotokoll)
SAN	Storage Area Network (Speichernetz)
SDH	Synchronous Digital Hierarchy (synchrone digitale Hierarchie)
SIS II	Schengener Informationssystem der zweiten Generation
SMTP	Simple Mail Transport Protocol (einfaches Mailübertragungsprotokoll)
SNMP	Simple Network Management Protocol (einfaches Netzverwaltungsprotokoll)
s-TESTA	Secure Trans-European Services for Telematics between Administrations (gesicherte transeuropäische Telematikdienste für Behörden), eine Maßnahme des Programms IDABC (Interoperable delivery of pan-European eGovernment services to public administrations, business and citizens — Interoperable Erbringung europaweiter elektronischer Behördendienste (E-Government-Dienste) für öffentliche Verwaltungen, Unternehmen und Bürger, Beschluss 2004/387/EG des Europäischen Parlaments und des Rates vom 21.4.2004)
TCP	Transmission Control Protocol (Übertragungskontrollprotokoll)
VIS	Visa-Informationssystem
VPN	Virtual Private Network (virtuelles privates Netz)
WAN	Wide Area Network (Weitverkehrsnetz)

2. **Allgemeiner Überblick**

Das SIS II besteht aus:

— einem zentralen System (nachstehend „zentrales SIS II“ genannt), zu dem folgende Elemente gehören:

• ein System zur technischen Unterstützung (nachstehend „CS-SIS“ genannt), das die SIS-II-Datenbank enthält; das Haupt-CS-SIS wird für die technische Überwachung und die Systemverwaltung eingesetzt, und das Backup-CS-SIS kann alle Funktionalitäten des Haupt-CS-SIS bei einem Ausfall dieses Systems übernehmen;

• eine einheitliche nationale Schnittstelle (nachstehend „NI-SIS“ genannt);

— einem nationalen Teil (nachstehend „N.SIS II“ genannt) in jedem einzelnen Mitgliedstaat, der sich aus den nationalen EDV-Systemen zusammensetzt, die Daten mit dem zentralen SIS II austauschen. Jeder N.SIS II kann in einer Datei (nachstehend „nationale Kopie“ genannt) den vollständigen Datenbestand der SIS-II-Datenbank oder einen Teil davon enthalten;

— einer Infrastruktur für die Kommunikation zwischen dem CS-SIS und der NI-SIS (nachstehend „Kommunikationsinfrastruktur“ genannt), die ein verschlüsseltes virtuelles Netz speziell für SIS-II-Daten und den Austausch von Daten zwischen SIRENE-Büros bietet.

Die NI-SIS besteht aus:

— einer lokalen nationalen Schnittstelle (nachstehend „LNI“ genannt) in jedem Mitgliedstaat, über die die Mitgliedstaaten physisch an das sichere Kommunikationsnetz angeschlossen sind und die die Verschlüsselungssysteme für den Datenverkehr von SIS II und SIRENE enthält. Die LNI befindet sich an Standorten in den Mitgliedstaaten;

— einer optionalen lokalen nationalen Backup-Schnittstelle (nachstehend „BLNI“ genannt), die inhaltlich und funktionsmäßig der LNI entspricht.

Die LNI und die BLNI werden ausschließlich für das SIS-II-System und den Austausch zwischen SIRENE-Büros genutzt. Die Konfiguration der LNI und der BLNI wird mit jedem und für jeden Mitgliedstaat vereinbart, um den Sicherheitsanforderungen, der physischen Umgebung und den Installationsbedingungen, darunter den Diensten des Netzanbieters, Rechnung tragen zu können; das bedeutet, dass der s-TESTA-Anschluss mehrere VPN-Tunnel für andere Systeme, beispielsweise für das VIS und Eurodac, umfassen kann;

— Die LNI und die BLNI werden ausschließlich für das SIS-II-System und den Austausch zwischen SIRENE-Büros genutzt. Die Konfiguration der LNI und der BLNI wird mit jedem und für jeden Mitgliedstaat vereinbart, um den Sicherheitsanforderungen, der physischen Umgebung und den Installationsbedingungen, darunter den Diensten des Netzanbieters, Rechnung tragen zu können; das bedeutet, dass der s-TESTA-Anschluss mehrere VPN-Tunnel für andere Systeme, beispielsweise für das VIS und Eurodac, umfassen kann;

Zur Infrastruktur für die Kommunikation zwischen dem CS-SIS und der NI-SIS gehören folgende Elemente:

— das Netz für gesicherte transeuropäische Telematikdienste für Behörden (nachstehend „s-TESTA“ genannt), ein verschlüsseltes virtuelles privates Netz ausschließlich für den Austausch von SIS-II-Daten und SIRENE-Daten.

3. **Geografische Reichweite**

Die Kommunikationsinfrastruktur muss sämtliche Mitgliedstaaten erfassen und die erforderlichen Dienste anbieten können:

sämtliche EU-Staaten (Belgien, Frankreich, Deutschland, Luxemburg, die Niederlande, Italien, Portugal, Spanien, Griechenland, Österreich, Dänemark, Finnland, Schweden, Zypern, die Tschechische Republik, Estland, Ungarn, Lettland, Litauen, Malta, Polen, die Slowakei, Slowenien, das Vereinigte Königreich und Irland) sowie Norwegen, Island und die Schweiz.

Darüber hinaus muss das System auch auf die Beitrittsländer Rumänien und Bulgarien ausgedehnt werden können.

Die Kommunikationsinfrastruktur muss schließlich auch andere Länder oder Stellen erfassen können, die sich dem zentralen SIS II anschließen (z. B. Europol, Eurojust).

4. **Netzdienste**

Gleichwertige künftige Technologien, Protokolle und Architekturen zu jedem genannten Protokoll und jeder Architektur müssen akzeptabel sein.

4.1. *Netzaufbau*

Bei der SIS-II-Architektur werden zentrale Dienste genutzt, auf die von den Mitgliedstaaten aus zugegriffen werden kann. Aus Gründen der Systemstabilität sind diese zentralen Dienste an zwei Standorten, nämlich im französischen Straßburg (das CS-SIS, CU) und im österreichischen St. Johann im Pongau (das Backup-CS-SIS, BCU) angesiedelt.

Der Zugang zu den aus dem Hauptsystem bestehenden zentralen Einheiten (Central Unit — CU) und dem Backup-System (BCU) muss von den Mitgliedstaaten aus möglich sein. Die beteiligten Staaten können mehrere Netzzugangspunkte, eine LNI und eine BLNI, zum Anschluss ihres nationalen Systems an die zentralen Dienste haben.

Neben dieser Anschlussmöglichkeit an die zentralen Dienste muss die Kommunikationsinfrastruktur zudem auch den bilateralen Austausch zusätzlicher Daten zwischen den SIRENE-Büros der Mitgliedstaaten ermöglichen.

4.2. *Art der Verbindung zwischen dem Haupt-CS-SIS und dem Backup-CS-SIS*

Um eine Zusammenschaltung des Haupt-CS-SIS und des Backup-CS-SIS zu ermöglichen, bedarf es einer SDH-Ring oder entsprechenden Struktur, also einer Verbindung, die auch für neue Architekturen und Technologien geeignet ist. Die SDH-Infrastruktur wird verwendet, um die lokalen Netze beider zentraler Systeme zu einem einzigen nahtlosen lokalen Netz (LAN) zu verbinden. Dieses LAN wird dann zur laufenden Synchronisierung von CU und BCU genutzt.

4.3. *Bandbreite*

Ein wichtiger Parameter der Kommunikationsinfrastruktur ist die Bandbreite, die sie den einzelnen angeschlossenen Systemen bietet. Auch das Backbone-Netz muss auf diese Bandbreite ausgelegt sein.

Für die LNI und die optionale BLNI wird in jedem Mitgliedstaat eine andere Bandbreite nötig sein, je nachdem, ob sich dieser für nationale Kopien, die Suche im zentralen System oder den Austausch biometrischer Daten entschieden hat.

Wie groß die Bandbreite, die die Kommunikationsinfrastruktur bietet, letztendlich ist, ist nicht entscheidend, vorausgesetzt, sie genügt den Mindestanforderungen jedes Mitgliedstaates.

Jede der genannten Arten von Netzstellen kann große Datenmengen (alphanumerische und biometrische Daten sowie ganze Dokumente) hoch und herunterladen. Daher muss die Kommunikationsinfrastruktur für jede Verbindung eine Mindestübertragungsrate für das Hoch und Herunterladen garantieren.

Die Kommunikationsinfrastruktur muss eine Datenübertragungsrate von 2 Mbps bis 155 Mbps oder mehr gewährleisten. Das Netz muss eine ausreichende garantierte Übertragungsrate für das Herunter und Hochladen für jede Verbindung bieten und auf die gesamte Bandbreite der Netzzugangspunkte ausgelegt sein.

4.4. *Dienstkategorien*

Im zentralen SIS II können für Anfragen/Ausschreibungen Prioritäten festgelegt werden. Daher muss die Kommunikationsinfrastruktur auch eine Prioritätenvergabe für den Datenverkehr ermöglichen.

Die Parameter für die Prioritätenvergabe im Netz werden für alle Pakete, für die eine Priorität vergeben werden muss, vom zentralen SIS II festgelegt. Dazu wird die WFQ-Technik (Weighted Fair Queuing) verwendet. Die Kommunikationsinfrastruktur muss somit in der Lage sein, die den Datenpaketen zugewiesenen Prioritäten des Quellen-LAN zu übernehmen und die Pakete im eigenen Backbone-Netz entsprechend zu behandeln. Außerdem muss die Kommunikationsinfrastruktur über eine Remote-Verbindung die ursprünglichen Datenpakete mit den Prioritäten übermitteln, die ihnen im Quellen-LAN zugewiesen wurden.

4.5. *Vorgesehene Protokolle*

Das zentrale SIS II wird verschiedene Netzkommunikationsprotokolle verwenden. Die Kommunikationsinfrastruktur sollte auf ein breites Spektrum von Netzkommunikationsprotokollen ausgelegt sein. Die Nutzung der Standardprotokolle HTTP, FTP, NTP, SMTP, SNMP und DNS ist vorgesehen.

Neben den Standardprotokollen muss die Kommunikationsinfrastruktur auch für verschiedene Tunnel-Protokolle, SAN-Replikationsprotokolle und die proprietären Verbindungsprotokolle für die Verbindung von zwei Java-Datenbanken von BEA WebLogic geeignet sein. Die Tunnelprotokolle, z. B. IPsec im Tunnelmodus, werden auch für die Übertragung von verschlüsselten Daten an die Bestimmungsadresse verwendet.

4.6. *Technische Spezifikationen*

4.6.1. IP-Adressierung

Der Kommunikationsinfrastruktur müssen verschiedene eindeutige IP-Adressen zugewiesen sein, die nur innerhalb dieses Netzes verwendet werden dürfen. Einige dieser IP-Adressen werden dem zentralen SIS II vorbehalten und dürfen auch nur hierfür verwendet werden.

4.6.2. Unterstützung für Ipv6

Es ist davon auszugehen, dass in den lokalen Netzen der Mitgliedstaaten das Protokoll TCP/IP verwendet wird, wobei an einigen Standorten Version 4 und an anderen Version 6 zugrunde gelegt wird. Die Netzzugangspunkte müssen als Gateway dienen können und unabhängig von den im zentralen SIS II sowie in den N.SIS II verwendeten Netzprotokollen operabel sein.

4.6.3. Statische Routenvorgabe

Die CU und die BCU können eine einzige identische IP-Adresse für die Kommunikation mit den Mitgliedstaaten verwenden. Die Kommunikationsinfrastruktur sollte daher für eine statische Routenvorgabe ausgelegt sein.

4.6.4. Konstanter Datendurchsatz

Solange der Datendurchsatz der CU- bzw. der BCU-Verbindung unter 90 % liegt, muss der jeweilige Mitgliedstaat kontinuierlich 100 % seiner Bandbreite aufrechterhalten können.

4.6.5. Sonstige Spezifikationen

Für das CS-SIS muss die Kommunikationsinfrastruktur mindestens folgenden technischen Spezifikationen entsprechen:

Die Übertragungsverzögerung darf (auch bei hoher Netzauslastung) 150 ms bei 95 % der Pakete und 200 ms bei 100 % der Pakete nicht übersteigen.

Die Wahrscheinlichkeit des Paketverlusts darf (auch bei hoher Netzauslastung) 10^{-4} bei 95 % der Pakete nicht übersteigen und muss unter 10^{-3} bei 100 % der Pakete liegen.

Die oben angegebenen Spezifikationen gelten gesondert für jeden Zugangspunkt.

Bei der Verbindung zwischen der CU und der BCU darf die Umlaufverzögerung 60 ms nicht übersteigen.

4.7. *Systemstabilität*

Das CS-SIS wurde mit der Vorgabe einer hohen Verfügbarkeit konzipiert. Zum Schutz gegen Fehlfunktionen einzelner Bestandteile ist das System daher durch Verdoppelung der gesamten Ausrüstung stabil auszulegen.

Die Kommunikationsinfrastruktur muss auch gegen den Ausfall von Bestandteilen abgesichert sein. Dies bedeutet, dass folgende Bestandteile stabil konzipiert sein müssen:

— Backbone-Netz;

— Router;

— Präsenzpunkte;

— Local-Loop-Verbindungen (einschließlich redundanter Verkabelung);

— Sicherheitsvorrichtungen (Verschlüsselungssysteme, Firewalls usw.);

— alle Basisdienste (DNS, NTP usw.);

— LNI/BLNI.

Die Failover-Mechanismen für die gesamte Netzausrüstung sollten ohne manuelles Zutun ausgelöst werden.

5. **Überwachung**

Damit eine einfachere Überwachung möglich ist, müssen die Überwachungsinstrumente der Kommunikationsinfrastruktur und diejenigen der Überwachungsvorrichtungen der Stelle, die für das Betriebsmanagement des zentralen SIS II zuständig ist, integriert werden können.

6. **Basisdienste**

Abgesehen von dem dedizierten Netz und den Sicherheitsdiensten muss die Kommunikationsinfrastruktur auch Basisdienste umfassen.

Dedizierte Dienste müssen zu Redundanzzwecken in beiden Zentraleinheiten implementiert werden.

Folgende optionale Basisdienste müssen Bestandteil der Kommunikationsinfrastruktur sein:

Dienst	Zusatzinformationen
DNS	Derzeit basiert das Failover-Verfahren für das Umschalten von der CU auf die BCU im Falle eines Netzausfalls auf der Änderung der IP-Adresse im generischen DNS-Server.
E-Mail-Relay	Die Verwendung eines generischen E-Mail-Relays könnte für die Standardisierung des E-Mail-Setups für die verschiedenen Mitgliedstaaten nützlich sein und verbraucht — im Gegensatz zu einem dedizierten Server — keine Netzressourcen der CU/BCU. Auch E-Mails, die über das generische E-Mail-Relay versandt werden, müssen die für sie geltenden Sicherheitsvorgaben (Sicherheitstemplate) erfüllen.
NTP	Dieser Dienst kann zur Synchronisierung der Uhren der Netzausrüstung verwendet werden.

7. **Verfügbarkeit**

Unabhängig von der Verfügbarkeit des Gesamtnetzes müssen das CS-SIS sowie die LNI und die BLNI für eine Verfügbarkeit von 99,99 % binnen eines beliebigen 28-Tage-Zeitraums ausgelegt sein.

Die Verfügbarkeit der Kommunikationsinfrastruktur muss ebenfalls 99,99 % betragen.

8. **Sicherheitsdienste**

8.1. *Netzverschlüsselung*

Das zentrale SIS II gestattet nicht, dass Daten, für die hohe bzw. sehr hohe Schutzvorgaben gelten, unverschlüsselt außerhalb des LAN übertragen werden. Es ist sicherzustellen, dass der Netzbetreiber in keinem Fall Zugriff auf die operativen SIS-II-Daten sowie auf den entsprechenden über SIRENE abgewickelten Datenaustausch hat.

Damit ständig ein hohes Maß an Sicherheit gewährleistet ist, muss die Kommunikationsinfrastruktur die Verwaltung der Zertifikate/Schlüssel ermöglichen. Die Fernverwaltung und Fernüberwachung der Verschlüsselungsboxen muss möglich sein. Für die Verschlüsselungsalgorithmen gelten folgende Mindestanforderungen:

— Symmetrische Verschlüsselungsalgorithmen:

• 3DES (128 Bit) oder besser;

• die Schlüsselerzeugung muss auf Zufallswerten basieren, die im Falle eines Angriffs keine Schlüsselverkürzung zulassen;

• die Verschlüsselungsschlüssel oder Informationen, anhand deren sich die Schlüssel ableiten lassen könnten, müssen bei der Speicherung stets geschützt sein.

— Asymmetrische Verschlüsselungsalgorithmen:

• RSA (1 024-Bit-Modul) oder besser;

• die Schlüsselerzeugung muss auf Zufallswerten basieren, die im Falle eines Angriffs keine Schlüsselverkürzung zulassen.

Das ESP-Protokoll (Encapsulated Security Payload — ESP, RFC2406) ist im Tunnelmodus zu verwenden. Der Payload-Header und der ursprüngliche IP-Header sind zu verschlüsseln.

Zum Austausch der Sitzungsschlüssel ist das IKE-Protokoll (Internet Key Exchange — IKE) zu verwenden.

IKE-Schlüssel dürfen nicht länger als einen Tag gültig sein.

Sitzungsschlüssel dürfen nicht länger als eine Stunde gültig sein.

8.2. *Sonstige Sicherheitsmerkmale*

Die Kommunikationsinfrastruktur muss so ausgelegt sein, dass nicht nur die SIS-II-Zugangspunkte, sondern auch die optionalen Basisdienste geschützt werden. Für diese Dienste sollten vergleichbare Schutzmaßnahmen wie für das CS-SIS getroffen werden. Alle Basisdienste müssen daher mindestens durch eine Firewall sowie eine Antivirus- und eine Angriffserkennungssoftware geschützt werden. Außerdem sollten die Geräte für die Basisdienste und die diesbezüglichen Schutzmaßnahmen einer ständigen Sicherheitsüberwachung (Logging und Follow-up) unterzogen werden.

Damit kontinuierlich ein hohes Maß an Sicherheit gewährleistet ist, muss die für das Betriebsmanagement des zentralen SIS II zuständige Stelle über alle Sicherheitsvorfälle innerhalb der Kommunikationsinfrastruktur informiert sein. Die Kommunikationsinfrastruktur muss also ermöglichen, dass alle schwerwiegenden Sicherheitsvorfälle unverzüglich der für die operative Verwaltung des zentralen SIS II verantwortlichen Einrichtung gemeldet werden.

9. **Helpdesk und Unterstützungsstruktur**

Der Anbieter der Kommunikationsinfrastruktur muss ein Helpdesk bereitstellen, das mit der für das Betriebsmanagement des zentralen SIS II zuständigen Stelle interagiert.

10. **Interaktion mit anderen Systemen**

Die Kommunikationsinfrastruktur muss gewährleisten, dass die Informationen ausschließlich über die zugewiesenen Kommunikationskanäle weitergeleitet werden können. In technischer Hinsicht setzt dies voraus, dass

— jeglicher unbefugte und/oder unkontrollierte Zugang zu anderen Netzen und die Vernetzbarkeit mit dem Internet streng untersagt sind;

— keine Daten in andere Systeme des Netzes entweichen dürfen, d. h. das Zusammenschalten verschiedener IP-VPNs ist nicht gestattet.

Abgesehen von den oben genannten technischen Einschränkungen ergeben sich auch Auswirkungen für das Helpdesk der Kommunikationsinfrastruktur. Das Helpdesk darf Informationen, die das zentrale SIS II betreffen, nur an die für das Betriebsmanagement des zentralen SIS II zuständige Stelle weiterleiten.