II

(Retsakter vedtaget i henhold til traktaterne om oprettelse af Det Europæiske Fællesskab/Euratom, hvis offentliggørelse ikke er obligatorisk)

AFGØRELSER OG BESLUTNINGER

KOMMISSIONEN

KOMMISSIONENS BESLUTNING

af 16. marts 2007

om fastsættelse af netværkskravene til Schengen II-informationsssystemet (første søjle)

(meddelt under nummer K(2007) 845)

(Kun den bulgarske, den estiske, den finske, den franske, den græske, den italienske, den lettiske, den litauiske, den maltesiske, den nederlandske, den polske, den portugisiske, den rumænske, den slovakiske, den slovenske, den spanske, den svenske, den tjekkiske, den tyske, og den ungarske udgave er autentiske)

(2007/170/EF)

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab,

under henvisning til Rådets forordning (EF) nr. 2424/2001 af 6. december 2001 om udvikling af anden generation af Schengen-informationssystemet (SIS II) [1], særlig artikel 4, litra a), og

ud fra følgende betragtninger:

(1) For at udvikle SIS II er det nødvendigt at fastsætte tekniske specifikationer for kommunikationsnettet og dets komponenter samt specifikke netværkskrav.

(2) Der bør indføres passende ordninger mellem Kommissionen og medlemsstaterne, navnlig for så vidt angår elementerne i den ensartede nationale grænseflade i medlemsstaterne.

(3) Denne beslutning har ingen indflydelse på vedtagelsen fremover af andre kommissionsbeslutninger vedrørende udviklingen af SIS II, navnlig udviklingen af sikkerhedskravene.

(4) Såvel forordning (EF) nr. 2424/2001 som Rådets afgørelse 2001/886/RIA [2] indeholder bestemmelser for udviklingen af SIS II. For at sikre, at der bliver én enkelt gennemførelseprocedure for udviklingen af SIS II som helhed, bør bestemmelserne i denne beslutning svare til bestemmelserne i Kommissionens afgørelse om fastsættelse af netværkskrav til SIS II, som skal vedtages i medfør af afgørelse 2001/886/RIA.

(5) I medfør af Rådets afgørelse 2000/365/EF af 29. maj 2000 om anmodningen fra Det Forenede Kongerige Storbritannien og Nordirland om at deltage i visse bestemmelser i Schengen-reglerne [3] har Det Forenede Kongerige ikke deltaget i vedtagelsen af forordning (EF) nr. 2424/2001, som ikke er bindende for og ikke finder anvendelse i Det Forenede Kongerige, da den udgør en udvikling af bestemmelser i Schengen-reglerne. Denne kommissionsbeslutning er derfor ikke rettet til Det Forenede Kongerige.

(6) I medfør af Rådets afgørelse 2002/192/EF af 28. februar 2002 om anmodningen fra Irland om at deltage i visse bestemmelser i Schengen-reglerne [4] har Irland ikke deltaget i vedtagelsen af forordning (EF) nr. 2424/2001, som ikke er bindende for og ikke finder anvendelse i Irland, da den udgør en udvikling af bestemmelser i Schengen-reglerne. Denne kommissionsbeslutning er derfor ikke rettet til Irland.

[1] EFT L 328 af 13.12.2001, s. 4. Ændret ved forordning (EF) nr. 1988/2006 (EUT L 411 af 30.12.2006, s. 1).

[2] EFT L 328 af 13.12.2001, s. 1.

[3] EFT L 131 af 1.6.2000, s. 43. Ændret ved afgørelse 2004/926/EF (EUT L 395 af 31.12.2004, s. 70).

[4] EFT L 64 af 7.3.2002, s. 20.

(7) I henhold til artikel 5 i protokollen om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og traktaten om oprettelse af Det Europæiske Fællesskab, har Danmark besluttet at gennemføre forordning (EF) nr. 2424/2001 i dansk lovgivning. Forordning (EF) nr. 2424/2001 er således bindende for Danmark i international ret.

(8) For så vidt angår Island og Norge udgør forordning (EF) nr. 2424/2001 og afgørelse 2001/886/RIA en udvikling af bestemmelserne i Schengen-reglerne som omhandlet i den aftale, som Rådet for Den Europæiske Union har indgået med Republikken Island og Kongeriget Norge om disse to staters associering i gennemførelsen, anvendelsen og udviklingen af Schengen-reglerne [1], som falder inden for det område, der er omhandlet i artikel 1, litra B, i Rådets afgørelse 1999/437/EF af 17. maj 1999 om visse gennemførelsesbestemmelser til den aftale, som Rådet for Den Europæiske Union har indgået med Republikken Island og Kongeriget Norge om disse to staters associering i gennemførelsen, anvendelsen og den videre udvikling af Schengen-reglerne [2].

(9) For så vidt angår Schweiz udgør forordning (EF) nr. 2424/2001 og afgørelse 2001/886/RIA en udvikling af Schengen-reglerne som omhandlet i aftalen mellem Den Europæiske Union, Det Europæiske Fællesskab og Det Schweiziske Forbund om Det Schweiziske Forbunds associering i gennemførelsen, anvendelsen og udviklingen af Schengen-reglerne, som falder inden for det område, der er omhandlet i artikel 4, stk. 1, i Rådets afgørelse om undertegnelse, på Det Europæiske Fællesskabs vegne, af og midlertidig anvendelse af visse bestemmelser i aftalen.

(10) Denne beslutning udgør en retsakt, der bygger på Schengen-reglerne eller på anden måde har tilknytning til dem i overensstemmelse med artikel 3, stk. 1, i tiltrædelsesakten.

(11) Foranstaltningerne i denne beslutning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 6, stk. 1, i forordning (EF) nr. 2424/2001 —

VEDTAGET FØLGENDE BESLUTNING:

Artikel 1

De tekniske specifikationer vedrørende udformningen af den fysiske arkitektur for SIS II-kommunikationsinfrastrukturen er som fastsat i bilaget.

Artikel 2

Denne beslutning er rettet til Kongeriget Belgien, Republikken Bulgarien, Den Tjekkiske Republik, Forbundsrepublikken Tyskland, Republikken Estland, Den Hellenske Republik, Kongeriget Spanien, Den Franske Republik, Den Italienske Republik, Republikken Cypern, Republikken Letland, Republikken Litauen, Storhertugdømmet Luxembourg, Republikken Ungarn, Republikken Malta, Kongeriget Nederlandene, Republikken Østrig, Republikken Polen, Den Portugisiske Republik, Rumænien, Republikken Slovenien, Den Slovakiske Republik, Republikken Finland og Kongeriget Sverige.

Udfærdiget i Bruxelles, den 16. marts 2007.

På Kommissionens vegne

Franco FRATTINI

Næstformand

[1] EFT L 176 af 10.7.1999, s. 36.
[2] EFT L 176 af 10.7.1999, s. 31.

BILAG

INDHOLDSFORTEGNELSE

1. Indledning

I dette dokument beskrives udformningen af kommunikationsnettet, dets komponenter og de specifikke netværkskrav.

1.1. *Akronymer og forkortelser*

I dette afsnit redegøres der for de i dokumentet anvendte akronymer og forkortelser.

Akronymer og forkortelser	Forklaring
BLNI	Backup Local National Interface (backup af den lokale nationale grænseflade)
CEP	Central End Point
CNI	Central National Interface (central national grænseflade)
CS	Central System (det centrale system)
CS-SIS	Teknisk støttefunktion, der indeholder SIS II-databasen
DNS	Domain Name Server
FCIP	Fibre Channel over IP
FTP	File Transport Protocol (filoverførselsprotokol)
HTTP	Hyper Text Transfer Protocol (protokol for hypertekstoverførsel)
IP	Internetprotokol
LAN	Local Area Network
LNI	Local National Interface (lokal national grænseflade)
Mbps	Megabits pr. sekund
MDC	Main Developer Contractor
N.SIS II	Den nationale del i hver medlemsstat
NI-SIS	En ensartet national grænseflade
NTP	Network Time Protocol (protokol for netværkstid)
SAN	Storage Area Network (lagringsnetværk)
SDH	Synchronous Digital Hierarchy
SIS II	Schengen-informationssystemet, anden generation
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
S-Testa	Sikre transeuropæiske telematiktjenester mellem administrationer er en foranstaltning under Idabc-programmet (interoperabel levering af paneuropæiske e-forvaltningstjenester til offentlige myndigheder, virksomheder og borgere. Europa-Parlamentets og Rådets afgørelse 2004/387/EF af 21.4.2004).
TCP	Transmission Control Protocol
VIS	Visuminformationssystemet
VPN	Virtual Private Network (virtuelt privat net)
WAN	Wide Area Network

2. **Generel oversigt**

SIS II består af:

— det centrale system (det centrale SIS II), der består af:

  • en teknisk støttefunktion (CS-SIS), der indeholder SIS II-databasen. Via CS-SIS-funktionen udføres det tekniske tilsyn og forvaltningen, og en backup af CS-SIS er med til at sikre alle funktionaliteter i forbindelse med CS-SIS-funktionen, hvis sidstnævnte skulle svigte

  • en ensartet national grænseflade (NI-SIS).

— en national del (N.SIS II) i hver medlemsstat, der består af nationale datasystemer, der kommunikerer med den centrale SIS II. En N.SIS II kan indeholde en datafil (national kopi), som indeholder en fuldstændig eller delvis kopi af SIS II-databasen

— en kommunikationsinfrastruktur mellem CS-SIS og NI-SIS (kommunikationsinfrastrukturen), der sikrer et krypteret virtuelt netværk forbeholdt SIS II-oplysninger og udvekslingen af oplysninger mellem Sirene-kontorer.

NI-SIS består af:

— en lokal national grænseflade (LNI) i hver medlemsstat, der er den grænseflade, hvorigennem medlemsstaten fysisk er forbundet med det sikre kommunikationsnetværk, og som indeholder krypteringsværktøjer med henblik på datatrafikken mellem SIS II og Sirene. LNI er placeret i medlemsstaterne

— en fakultativ backup af den lokale nationale grænseflade (BLNI), der har nøjagtig samme indhold og funktion som LNI.

LNI og BLNI skal udelukkende anvendes i forbindelse med SIS II-systemet og til udvekslinger mellem Sirene-kontorer. Den specifikke konfigurering af LNI og BLNI vil blive specificeret og aftalt med hver enkelt medlemsstat for at tage hensyn til sikkerhedskravene, den fysiske placering og installationsforholdene, herunder netudbyderens levering af ydelser; det betyder, at den fysiske S-Testa-opkobling kan indeholder flere VPN-tunneller til andre systemer, f.eks. VIS og Eurodac.

— en central national grænseflade (CNI), der er en applikation, der sikrer adgangen til CS-SIS. Hver medlemsstat har separate logiske adgangspunkter via en central firewall.

Kommunikationsinfrastrukturen mellem CS-SIS og NI-SIS består af:

— nettet for sikre transeuropæiske telematiktjenester mellem administrationer (S-Testa), der er et krypteret, virtuelt, privat net til udveksling af SIS II-data og Sirene-data.

3. **Geografisk dækning**

Kommunikationsinfrastrukturen skal kunne dække og levere de krævede tjenester til alle medlemsstater.

Alle EU-medlemsstater (Belgien, Tjekkiet, Danmark, Tyskland, Estland, Irland Grækenland, Spanien, Frankrig, Italien, Cypern, Letland, Litauen, Luxembourg, Ungarn, Malta, Nederlandene, Østrig, Polen, Portugal, Slovenien, Slovakiet, Finland, Sverige og Det Forenede Kongerige) samt Norge, Island og Schweiz.

Derudover skal der sikres dækning af tiltrædelseslandene Bulgarien og Rumænien.

Endelig skal kommunikationsinfrastrukturen kunne udvides til et hvilket som helst andet land eller en hvilken som helst anden enhed, der tilsluttes det centrale SIS II-system (f.eks. Europol eller Eurojust).

4. **Nettjenester**

Når der nævnes en protokol eller arkitektur, er det underforstået, at tilsvarende fremtidige teknologier, protokoller og arkitekturer også kan accepteres.

4.1. *Netarkitektur*

SIS II's arkitektur bygger på centraliserede tjenester, der er tilgængelige fra forskellige medlemsstater. Af hensyn til systemets stabilitet er disse centraliserede tjenester duplikeret to forskellige steder, nemlig i Strasbourg i Frankrig (CS-SIS, CU) og i St Johann i Pongau i Østrig (backuppen af CS-SIS, BCU).

De centrale enheder (hovedenheden og backuppen) skal være tilgængelige fra forskellige medlemsstater. De deltagende lande kan have flere netadgangspunkter, en LNI og en BLNI, for at koble deres nationale system til de centrale tjenester.

Ud over denne tilkoblingsmulighed til de centrale tjenester skal kommunikationsinfrastrukturen også understøtte bilaterale supplerende informationsudvekslinger mellem Sirene-kontorer i forskellige medlemsstater.

4.2. *Sammenkoblingstype mellem CS-SIS og backup-CS-SIS*

For at sammenkoble CS-SIS og backup-CS-SIS kræves der en SDH-ring eller tilsvarende, dvs. en type, der også er åben for nye fremtidige arkitekturer og teknologier. SDH-infrastrukturen vil blive anvendt til at udvide de lokale net for begge centrale enheder for derved at skabe et enkelt sømløst LAN. Dette LAN vil blive anvendt til løbende synkronisering af CU og BCU.

4.3. *Båndvidde*

Et vigtigt krav til kommunikationsinfrastrukturen er den båndvidde, den kan give de forskellige indbyrdes forbundne systemer, og at denne båndvidde også understøttes i dens eget backbonenet.

Båndvidden for LNI og den fakultative BLNI vil være forskellig for hver medlemsstat, afhængig af om medlemsstaten har besluttet at anvende nationale kopier, central søgning eller udveksling af biometriske data.

Kommunikationsinfrastrukturens reelle båndvidder er irrelevante, så længe de dækker hver medlemsstats minimumsbehov.

Via hver af de førnævnte netstedstyper kan der overføres store mængder data (alfanumeriske, biometriske og fuldstændige dokumenter) i hver retning. Kommunikationsinfrastrukturen skal derfor kunne yde og garantere tilstrækkelige mindstehastigheder for uploading og downloading ved hver tilkobling.

Kommunikationsinfrastrukturen skal kunne sikre dataoverførselsrater fra 2 Mbps til 155 Mbps eller mere. Nettet skal kunne sikre tilstrækkelige mindstehastigheder for uploading og downloading ved hver opkobling, og det skal være dimensioneret til at understøtte den samlede båndvidde for nettets adgangspunkter.

4.4. *Tjenestekategorier*

Via det centrale SIS II-system skal anmodninger/indberetninger kunne prioriteres. Kommunikationsinfrastrukturen skal som følge heraf også kunne støtte muligheden for at prioritere datatrafikken.

Parametrene for prioriteringen i nettet fastsættes i det centrale SIS II-system for alle pakker, der kræver det. Det vil ske ved hjælp af WFQ (Weighted Fair Queuing). Det indebærer, at kommunikationsinfrastrukturen skal kunne overtage den prioritering, der er fastsat for pakker, på LAN (kildenet) og behandle pakkerne herefter i sit eget backbonenet. Derudover skal kommunikationsinfrastrukturen på fjerne netsteder kunne formidle de oprindelige pakker, der har samme prioritering som i LAN.

4.5. *Understøttede protokoller*

I forbindelse med det centrale SIS II-system vil der blive anvendt flere netkommunikationsprotokoller, og kommunikationsinfrastrukturen skal understøtte en lang række netkommunikationsprotokoller. De standardprotokoller, der skal kunne understøttes, er HTTP, FTP, NTP, SMTP, SNMP og DNS.

Ud over standardprotokollerne skal kommunikationsinfrastrukturen også kunne understøtte forskellige tunnelprotokoller, SAN-replikationsprotokoller og proprietære Java til Java-forbindelsesprotokoller under BEA WebLogic. Tunnelprotokollerne, f.eks. IPsec i tunnelmodus, vil blive anvendt til at overføre krypterede data til bestemmelsesstedet.

4.6. *Tekniske specifikationer*

4.6.1. IP-adressering

Kommunikationsinfrastrukturen skal have en række reserverede IP-adresser, der kun kan anvendes inden for nettet. Nogle af disse IP-adresser vil være forbeholdt det centrale SIS II-system og må ikke anvendes andre steder.

4.6.2. Støtte til IPv6

Det kan antages, at den protokol, der anvendes på medlemsstaternes lokale net, vil være TCP/IP. På nogle vil version 4 blive anvendt, mens det på andre vil være version 6. Nettets adgangspunkter skal kunne fungere som gateways og skal kunne fungere uafhængigt af de netprotokoller, der anvendes i både det centrale SIS II-system og N.SIS II.

4.6.3. Statisk routing

CU og BCU kan anvende en enkelt identisk IP-adresse til kommunikationer til medlemsstaterne. Kommunikationsinfrastrukturen skal derfor understøtte statisk routing.

4.6.4. Konstant datatrafik

Så længe datatrafikken via CU- eller BCU-forbindelsen er på under 90 %, skal en given medlemsstat være i stand til hele tiden at opretholde 100 % af sin specificerede båndvidde.

4.6.5. Andre specifikationer

Med henblik på CS-SIS skal kommunikationsinfrastrukturen mindst opfylde følgende minimumssæt af tekniske specifikationer:

Overførselsforsinkelsen (også på spidsbelastningstidpunkter) skal være mindre end eller lig med 150 ms for 95 % af pakkerne og mindre end 200 ms for 100 % af pakkerne.

Sandsynligheden for tab af pakker skal (også på spidsbelastingstidspunkter) være mindre end eller lig med 10^{-4} for 95 % af pakkerne og mindre end 10^{-3} for 100 % af pakkerne.

Førnævnte specifikationer gælder særskilt for hvert adgangspunkt.

For forbindelsen mellem CU og BCU skal overførselstiden frem og tilbage være mindre end eller lig med 60 ms.

4.7. *Systemstabilitet*

Ved udformningen af CI-SIS var driftssikkerheden et krav. For at sikre systemets stabilitet og beskytte det mod, at visse komponenter fungerer dårligt, er alt udstyr duplikeret.

Kommunikationsinfrastrukturens komponenter skal også være beskyttet mod komponenter, der ikke virker. Det indebærer, at følgende komponenter skal være stabile:

— backbonenettet

— routingsystemer

— POP (Points of Presence)

— Local loop-forbindelser (herunder redundante kabelforbindelser)

— sikkerhedsværktøjer (krypteringsværktøjer, firewalls m.m.)

— alle basisydelser (DNS, NTP m.m.)

— LNI/BLNI.

Failover-mekanismen for alt netudstyr bør fungere uden manuel indgriben.

5. **Overvågning**

For at lette overvågningen skal kommunikationsinfrastrukturens overvågningsredskaber kunne integreres med de tilsvarende for overvågningsfaciliteterne for den organisation, der er ansvarlig for den operationelle drift af det centrale SIS II-system.

6. **Basistjenester**

Ud over de specialiserede net- og sikkerhedstjenester skal kommunikationsinfrastrukturen også kunne levere basistjenester.

Der skal af redundanshensyn være specialiserede tjenester i begge centrale enheder.

Kommunikationsinfrastrukturen skal omfatte følgende fakultative basistjenester:

Tjeneste	Supplerende oplysninger
DNS	På nuværende tidspunkt er failover-proceduren, hvor der skiftes fra CU til BCU i tilfælde af, at nettet går ned, baseret på en ændring af IP-adressen i den generiske DNS-server.
E-mail-relay	Det kan være nyttigt at anvende en videresendelse af generisk e-mail til standardisering af de forskellige medlemsstaters e-mail-opsætning, og i modsætning til en specifik server tager det ingen netressourcer fra CU/BCU. E-mails, der videresendes via den generiske e-mail, skal stadig være i overensstemmelse med deres sikkerhedstemplate.
NTP	Denne tjeneste kan anvenes til at synkronisere netudstyrets ure.

7. **Tilgængelighed**

Uafhængigt af nettets tilgængelighed skal CI-SIS og LNI og BLNI være 99,99 % tilgængelige over en 28-dages rulleperiode.

Kommunikationsinfrastrukturens tilgængelighed skal være på 99,99 %.

8. **Sikkerhedstjenester**

8.1. *Netkryptering*

Det centrale SIS II-system tillader ikke, at data med høje eller meget høje beskyttelseskrav bliver overført uden for LAN uden kryptering. Det bør sikres, at netudbyderen ikke på nogen måde har adgang til operationelle data i SIS II og til tilknyttede Sirene-udvekslinger.

For at opretholde et højt sikkerhedsniveau skal kommunikationsinfrastrukturen gøre det muligt at forvalte certifikater/nøgler. Fjernforvaltning og fjernovervågning af krypteringsbokse skal være mulig. Krypteringsalgoritmer skal mindst opfylde følgende krav:

— symmetriske krypteringsalgoritmer:

• 3DES (128 bits) eller bedre

• Nøglegenereringen skal baseres på tilfældige værdier, der i tilfælde af angreb ikke tillader mindskelse af nøglerummet.

• Krypteringsnøgler eller oplysninger, der kan anvendes til at derivere nøglerne, er altid beskyttet, når de er i »storage002E«.

— asymmetriske krypteringsalgoritmer:

• RSA (1 024 bit modulus) eller bedre

• Nøglegenereringen skal baseres på tilfældige værdier, der i tilfælde af angreb ikke tillader mindskelse af nøglerummet.

ESP-protokollen (Encapsulated Security Payload — ESP, RFC2406) skal anvendes, og det skal ske i tunnelmodus. Payload Headeren og den originale IP-header skal krypteres.

Til udskiftning af sessionsnøgler skal IKE-protokollen (Internet Key Exchange) anvendes.

IKE-nøgler må ikke være gyldige mere end én dag.

Sessionsnøgler må ikke være gyldige mere end én time.

8.2. *Andre sikkerhedskarakteristika*

Ud over at beskytte SIS II's adgangspunkter skal kommunikationsinfrastrukturen også beskytte de fakultative basistjenester. Disse bør omfattes af beskyttelsesforanstaltninger, der svarer til beskyttelsesforanstaltningerne i CS-SIS. Alle basistjenester skal derfor som et minimum beskyttes af en firewall, et antivirusprogram og et system, der forhindrer uautoriseret adgang til netværket. Derudover bør udstyret i forbindelse med basistjenester og beskyttelsesforanstaltninger være under løbende sikkerhedsovervågning (logning og follow-up).

For at bevare et højt sikkerhedsniveau skal den organisation, der er ansvarlig for den operationelle forvaltning af det centrale SIS II-system, være opmærksom på alle sikkerhedssvigt i kommunikationsinfrastrukturen. Kommunikationsinfrastrukturen skal derfor tillade, at alle sikkerhedssvigt straks indberettes til den organisation, der er ansvarlig for den operationelle forvaltning af det centrale SIS II-system. Alle sikkerhedssvigt skal indberettes regelmæssigt, f.eks. hver måned, og på ad hoc-basis.

9. **Helpdesk og støttestruktur**

Udbyderen af kommunikationsinfrastrukturen skal stille en helpdesk til rådighed, der samarbejder med den organisation, der er ansvarlig for den operationelle drift af det centrale SIS II-system.

10. **Interaktion med andre systemer**

Kommunikationsinfrastrukturen skal sikre, at oplysninger ikke kan komme uden for de fastsatte kommunikationskanaler. Med hensyn til den tekniske gennemførelse indebærer det, at:

— al uautoriseret og/eller ukontrolleret adgang til andre net er strengt forbudt, inklusive internettet

— der ikke må lækkes oplysninger til andre systemer på nettet; f.eks. er indbyrdes sammenkobling af forskellige IP-VPN'er ikke tilladt.

Ud over førnævnte tekniske begrænsninger har det også indvirkning på kommunikationsinfrastrukturens helpdesk. Helpdesken må ikke frigive oplysninger vedrørende det centrale SIS II-system til nogen som helst anden end den ansvarlige for den operationelle drift af det centrale SIS II-system.