II

*(Rättsakter som antagits i enlighet med EG- och Euratomfördragen och vars offentliggörande inte är obligatoriskt)*

# BESLUT

# KOMMISSIONEN

## KOMMISSIONENS BESLUT

**av den 16 mars 2007**

**om fastställande av nätkrav för Schengens informationssystem II (första pelaren)**

*[delgivet med nr K(2007) 845]*

**(Endast de bulgariska, estniska, finska, franska, grekiska, italienska, lettiska, litauiska, maltesiska, nederländska, polska, portugisiska, rumänska, slovakiska, slovenska, spanska, svenska, tjeckiska, tyska och ungerska texterna är giltiga)**

(2007/170/EG)

EUROPEISKA GEMENSKAPERNAS KOMMISSION HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om upprättandet av Europeiska gemenskapen,

med beaktande av rådets förordning (EG) nr 2424/2001 av den 6 december 2001 om utvecklingen av andra generationen av Schengens informationssystem (SIS II) [1], särskilt artikel 4 a, och

av följande skäl:

(1) För att utveckla SIS II är det nödvändigt att fastställa tekniska specifikationer för kommunikationsnätet, dess komponenter och de specifika nätkraven.

(2) Erforderliga samarbetsformer bör inrättas mellan kommissionen och medlemsstaterna, särskilt när det gäller delarna i det enhetliga nationella gränssnittet i medlemsstaterna.

(3) Det här beslutet påverkar inte antagandet av kommande kommissionsbeslut som rör utvecklingen av SIS II, i synnerhet beslut om framtagande av säkerhetskrav.

(4) Både förordning (EG) nr 2424/2001 och rådets beslut 2001/886/RIF [2] reglerar utvecklingen av SIS II. För att säkerställa en gemensam genomförandeprocess för utvecklingen av SIS II som helhet bör bestämmelserna i det här beslutet följa bestämmelserna i kommissionens beslut om fastställande av nätkraven för SIS II, som skall antas för tillämpningen av beslut 2001/886/RIF.

(5) I enlighet med rådets beslut 2000/365/EG av den 29 maj 2000 om en begäran från Förenade konungariket Storbritannien och Nordirland om att få delta i vissa bestämmelser i Schengenregelverket [3], har Förenade kungariket inte deltagit i antagandet av förordning (EG) nr 2424/2001 som därför inte är bindande för eller tillämplig i Förenade kungariket eftersom den utgör en utveckling av bestämmelser i Schengenregelverket. Detta kommissionsbeslut riktar sig därför inte till Förenade kungariket.

(6) I enlighet med rådets beslut 2002/192/EG av den 28 februari 2002 om en begäran från Irland om att få delta i vissa bestämmelser i Schengenregelverket [4], har Irland inte deltagit i antagandet av förordning (EG) nr 2424/2001 som därför inte är bindande för eller tillämplig i Irland eftersom den utgör en utveckling av bestämmelser i Schengenregelverket. Detta kommissionsbeslut riktar sig därför inte till Irland.

[1] EGT L 328, 13.12.2001, s. 4. Förordningen ändrad genom förordning (EG) nr 1988/2006 (EUT L 411, 30.12.2006, s. 1).

[2] EGT L 328, 13.12.2001, s. 1.

[3] EGT L 131, 1.6.2000, s. 43. Beslutet ändrat genom beslut 2004/926/EG (EUT L 395, 31.12.2004, s. 70).

[4] EGT L 64, 7.3.2002, s. 20.

(7) I enlighet med artikel 5 i protokollet om Danmarks ställning, som är fogat till fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, har Danmark beslutat att införliva rådets förordning (EG) nr 2424/2001 med dansk lagstiftning. Enligt internationell rätt är förordning (EG) nr 2424/2001 därför bindande för Danmark.

(8) När det gäller Island och Norge innebär förordning (EG) nr 2424/2001 och beslut 2001/886/RIF – i den mening som avses i avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket [1] – en utveckling av bestämmelser i Schengenregelverket vilka rör det område som avses i artikel 1.B i rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtal som har ingåtts mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket [2].

(9) När det gäller Schweiz utgör förordning (EG) nr 2424/2001 och beslut 2001/886/RIF – i den mening som avses i avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket – en utveckling av de bestämmelser i Schengenregelverket vilka rör det område som avses i artikel 4.1 i rådets beslut om undertecknande på Europeiska gemenskapens vägnar och provisorisk tillämpning av vissa bestämmelser i det avtalet.

(10) Detta beslut utgör en rättsakt som bygger på Schengenregelverket eller som på annat sätt hänför sig till det regelverket i den mening som avses i artikel 3.1 i anslutningsakten.

(11) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 6.1 i förordning (EG) nr 2424/2001.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

*Artikel 1*

De tekniska specifikationerna avseende utformningen av den fysiska arkitekturen i kommunikationsinfrastrukturen för SIS II fastställs i bilagan.

*Artikel 2*

Det här beslutet riktar sig till Konungariket Belgien, Republiken Bulgarien, Republiken Tjeckien, Förbundsrepubliken Tyskland, Republiken Estland, Republiken Grekland, Konungariket Spanien, Republiken Frankrike, Republiken Italien, Republiken Cypern, Republiken Lettland, Republiken Litauen, Storhertigdömet Luxemburg, Republiken Ungern, Republiken Malta, Konungariket Nederländerna, Republiken Österrike, Republiken Polen, Republiken Portugal, Rumänien, Republiken Slovenien, Republiken Slovakien, Republiken Finland och Konungariket Sverige.

Utfärdat i Bryssel den 16 mars 2007.

*På kommissionens vägnar*

Franco FRATTINI

*Vice ordförande*

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

*BILAGA*

**INNEHÅLLSFÖRTECKNING**

## 1. **Inledning**

I det här dokumentet beskrivs utformningen av kommunikationsnätet, dess komponenter och de specifika nätkraven.

### 1.1 *Förkortningar*

I det här avsnittet förklaras de förkortningar som används i dokumentet.

| Förkortningar | Förklaring |
|---|---|
| BLNI | *Backup Local National Interface* (backup av lokal nationellt gränssnitt) |
| CEP | *Central End Point* |
| CNI | *Central National Interface* (centralt nationellt gränssnitt) |
| CS | *Central System* (det centrala systemet) |
| CS-SIS | Teknisk stödfunktion som innehåller SIS II-databasen |
| DNS | *Domain Name Server* (domännamnsserver) |
| FCIP | *Fibre Channel over IP* |
| FTP | *File Transfer Protocol* |
| http | *Hyper Text Transfer Protocol* |
| IP | *Internet Protocol* (internetprotokoll) |
| LAN | *Local Area Network* (lokalt nät) |
| LNI | *Local National Interface* (lokalt nationellt gränssnitt) |
| Mbps | Megabit per sekund |
| MDC | *Main Developer Contractor* |
| N.SIS II | Main Developer Contractor |
| NI-SIS | Enhetligt nationellt gränssnitt |
| NTP | *Network Time Protocol* |
| SAN | *Storage Area Network* (lagringsnät) |
| SDH | *Synchronous Digital Hierarchy* |
| SIS II | Schengens informationssystem, andra generationen |
| SMTP | *Simple Mail Transport Protocol* |
| SNMP | *Simple Network Management Protocol* |
| s-TESTA | *Secure Trans-European Services for Telematics between Administrations* (säkra transeuropeiska telematiktjänster för myndigheter): en del av IDABC-programmet (*Interoperable delivery of pan-European eGovernment services to public administrations, business and citizens* – interoperabelt tillhandahållande av alleuropeiska e-förvaltningstjänster för offentliga förvaltningar, företag och medborgare. Europaparlamentets och rådets beslut 2004/387/EG av den 21 april 2004). |
| TCP | *Transmission Control Protocol* |
| VIS | *Visa Information System* (Informationssystemet för viseringar) |
| VPN | *Virtual Private Network* (virtuellt privat nät) |
| WAN | *Wide Area Network* |

2. **Översikt**

SIS II består av följande delar:

— Ett centralt system (nedan kallat ”SIS II-centralen”) bestående av följande:

  • En teknisk stödfunktion (nedan kallad ”CS-SIS”) som innehåller SIS II-databasen. En ordinarie CS-SIS står för teknisk tillsyn och administration, och en backup-CS-SIS kan ta över alla funktioner som normalt utförs av ordinarie CS-SIS om den skulle sluta fungera.

  • Ett enhetligt nationellt gränssnitt (nedan kallat ”NI-SIS”).

— En nationell del (nedan kallad ”N.SIS II”) i var och en av medlemsstaterna bestående av de nationella datasystem som står i förbindelse med SIS II-centralen. En N.SIS II kan innehålla en datafil (nedan kallad ”nationell kopia”) med en kopia av hela SIS II-databasen eller delar av den.

— En kommunikationsinfrastruktur som förenar CS-SIS och NI-SIS (nedan kallad ”kommunikationsinfrastruktur”) och som tillhandahåller ett krypterat virtuellt nät speciellt avsett för SIS II-data och utbytet av data mellan Sirenekontoren.

NI-SIS består av följande delar:

— Ett lokalt nationellt gränssnitt (nedan kallat ”LNI”) i varje medlemsstat. Det är det gränssnitt som fysiskt förbinder medlemsstaten med det säkra kommunikationsnätet, och det innehåller den krypteringsutrustning som är speciellt avsedd för SIS II-data och Sirenetrafik. LNI är lokaliserat till respektive medlemsstat.

— En backup-LNI som tillval (nedan kallat ”BLNI”) med exakt samma innehåll och funktion som LNI.

LNI och BLNI skall användas uteslutande av SIS II-systemet och för datautbyte mellan Sirenekontor. Konfigurationerna för LNI och BLNI kommer att fastställas för och överenskommas med varje enskild medlemsstat med beaktande av säkerhetskrav, fysisk placering och installationsförhållanden, däribland de tjänster som tillhandahålls av nätoperatören. Det betyder att den fysiska s-TESTA-förbindelsen kan innehålla flera VPN-tunnlar för andra system, t.ex. VIS och Eurodac.

— Ett centralt nationellt gränssnitt (nedan kallat ”CNI”) som är en tillämpning som ger tillträde till CS-SIS. Varje medlemsstat har separata logiska anslutningspunkter för anslutning till CNI via en central brandvägg.

Kommunikationsstrukturen som förenar CS-SIS och NI-SIS består av följande:

— Nätet för säkra transeuropeiska telematiktjänster för myndigheter (*Secure Trans-European Services for Telematics between Administrations* – nedan kallat ”s-TESTA”) som tillhandahåller ett krypterat, virtuellt privat nät som är speciellt avsett för SIS II-data och Sirenetrafik.

3. **Geografisk täckning**

Kommunikationsinfrastrukturen skall kunna täcka samt tillhandahålla erforderliga tjänster till alla medlemsstater:

Alla stater som är medlemmar i EU (Belgien, Tjeckien, Danmark, Tyskland, Irland, Estland, Grekland, Spanien, Frankrike, Italien, Cypern, Lettland, Litauen, Luxemburg, Ungern, Malta, Nederländerna, Österrike, Polen, Portugal, Slovenien, Slovakien, Finland, Sverige och Förenade kungariket) samt Norge, Island och Schweiz.

Dessutom skall man ordna täckning av anslutningsländerna Rumänien och Bulgarien.

Slutligen måste kommunikationsinfrastrukturen kunna utvidgas till andra länder eller organisationer som ansluter sig till SIS II-centralen (t.ex. Europol eller Eurojust).

4. **Nättjänster**

När ett protokoll eller en arkitektur nämns i detta dokument är det underförstått att likvärdiga framtida tekniska lösningar, protokoll och arkitekturer också är godtagbara.

4.1 *Nätutformning*

SIS II-arkitekturen använder centraliserade tjänster som är åtkomliga från de olika medlemsstaterna. Av stabilitetsskäl är dessa centraliserade tjänster dubblerade och återfinns på två olika platser, nämligen Strasbourg i Frankrike (ordinarie CS-SIS, CU) och St Johann im Pongau i Österrike (backup-CS-SIS, BCU).

Centralenheterna (*Central Unit*, CU), både huvudenhet och backup, måste vara åtkomliga från medlemsstaterna. De deltagande länderna kan ha flera nätanslutningspunkter, ett LNI och ett BLNI för anslutning av sina nationella system till de centrala tjänsterna.

Förutom att erbjuda dessa möjligheter för anslutning till de centrala tjänsterna skall kommunikationsinfrastrukturen också stödja bilateralt utbyte av tilläggsinformation mellan Sirenekontoren i de olika medlemsstaterna.

4.2 *Typ av förbindelse mellan ordinarie CS-SIS och backup-CS-SIS*

Förbindelsetypen för sammankoppling av ordinarie CS-SIS och backup-CS-SIS skall vara en SDH-ring eller ha motsvarande struktur, dvs. en förbindelsetyp som är öppen även för framtida arkitekturer och tekniska lösningar. SDH-infrastrukturen kommer att användas för att utvidga de lokala näten i båda centralenheterna så att det skapas ett enda sömlöst LAN. Detta LAN kommer sedan att användas för den kontinuerliga synkroniseringen mellan CU och BCU.

4.3 *Bandbredd*

Ett viktigt krav på kommunikationsinfrastrukturen är hur stor bandbredd den kan erbjuda de olika sammankopplade systemen och dess förmåga att stödja denna bandbredd inom sitt eget stomnät.

Den bandbredd som krävs för LNI och BLNI (tillval) kommer att vara olika för olika medlemsstater, huvudsakligen beroende på om medlemsstaten har valt att använda nationella kopior, central sökning och utbyte av biometriska data.

Hur stor bandbredd som kommunikationsinfrastrukturen faktiskt erbjuder är utan betydelse så länge den tillgodoser varje medlemsstats minimibehov.

Vart och ett av ovannämnda system kan överföra stora datamängder (alfanumeriska data, biometriska data samt fullständiga dokument) i båda riktningar. Därför måste kommunikationsinfrastrukturen tillhandahålla och garantera tillräckliga minsta upp- och nedladdningshastigheter för varje förbindelse.

Kommunikationsinfrastrukturen måste erbjuda överföringshastigheter från 2 Mbps upp till 155 Mbps eller högre. Nätet måste tillhandahålla och garantera tillräckliga minsta upp- och nedladdningshastigheter för varje förbindelse, och det måste vara dimensionerat så att det klarar nätanslutningspunkternas sammanlagda bandbredd.

4.4 *Tjänstekategorier*

SIS II-centralen kommer att kunna prioritera förfrågningar/registreringar (*queries/alerts*). Som en följd av detta kommer kommunikationsinfrastrukturen också att möjliggöra prioritering av trafiken.

Nätprioriteringsparametrarna antas fastställas av SIS II-centralen för alla paket som kräver detta. *Weighted Fair Queuing* kommer att användas. Det innebär att kommunikationsinfrastrukturen måste kunna överta den prioritering som tilldelats datapaketen i avsändande LAN och behandla paketen i enlighet med denna prioritering inom sitt eget stomnät. Dessutom måste kommunikationsinfrastrukturen leverera de ursprungliga paketen till mottagande system med samma prioritering som fastställdes i avsändande LAN.

4.5 *Protokoll*

SIS II-centralen kommer att använda flera nätkommunikationsprotokoll. Kommunikationsinfrastrukturen bör stödja ett brett spektrum av nätkommunikationsprotokoll. De standarprotokoll som skall stödjas är HTTP, FTP, NTP, SMTP, SNMP och DNS.

Utöver standardprotokollen skall kommunikationsinfrastrukturen kunna hantera olika tunnelprotokoll, protokoll för SAN-replikering (lagringsnät) och BEA WebLogics egenutvecklade protokoll för Java-till-Java-förbindelser. Tunnelprotokollen, t.ex. IPsec i tunnelmod, kommer att användas för överföring av krypterade data till destinationsadressen.

4.6 *Tekniska specifikationer*

4.6.1 IP-adressering

Kommunikationsinfrastrukturen skall ha en uppsättning reserverade IP-adresser som enbart får användas inom det nätet. Vissa av dessa IP-adresser kommer att vara reserverade för SIS II-centralen och får inte användas någon annanstans.

4.6.2 Stöd för IPv6

Det kan antas att protokollet i medlemsstaternas lokala nät kommer att vara TCP/IP. Vissa system kommer emellertid att bygga på version 4, medan andra kommer att bygga på version 6. Nätanslutningspunkterna skall kunna fungera som förmedlingsnoder och skall kunna fungera oberoende av de nätprotokoll som används i SIS II-centralen och i N.SIS II.

4.6.3 Statisk dirigering

CU och BCU kan använda en enda, identisk IP-adress för sin kommunikation med medlemsstaterna. Därför bör kommunikationsinfrastrukturen stödja statisk dirigering (*static route injection*).

4.6.4 Konstant dataflöde

Så länge CU- eller BCU-förbindelsen är belastad till mindre än 90 % måste den aktuella medlemsstaten kontinuerligt kunna upprätthålla 100 % av sin angivna bandbredd.

4.6.5 Övriga specifikationer

För att stödja CS-SIS måste kommunikationsinfrastrukturen som minimum uppfylla följande tekniska specifikationer:

Överföringsfördröjningen (även under tider med hög belastning) skall vara högst 150 ms för 95 % av paketen och mindre än 200 ms för 100 % av paketen.

Sannolikheten för paketförlust (även under tider med hög belastning) skall vara högst $10^{-4}$ för 95 % av paketen och mindre än $10^{-3}$ för 100 % av paketen.

Ovannämnda specifikationer skall gälla för var och en av anslutningspunkterna.

Överföringstiden tur- och retur (*round trip delay*) mellan CU och BCU skall vara högst 60 ms.

4.7 *Systemstabilitet*

CS-SIS har utformats med krav på hög tillgänglighet. All utrustning har därför dubblerats för att ge systemet integrerad stabilitet mot komponentfel.

Även komponenterna i kommunikationsinfrastrukturen måste vara stabila mot komponentfel. Det kräver stabilitet hos

— stomnätet,

— routrar,

— POP (*Points of Presence*),

— förbindelser till accessnät (inklusive fysiskt redundant kablage),

— säkerhetsutrustning (krypteringsutrustning, brandväggar etc.),

— alla bastjänster (DNS, NTP etc.),

— LNI och BLNI.

För all nätutrustning bör reservomkoppling till fungerande komponent (fail-over) ske utan manuellt ingripande.

5. **Övervakning**

För att underlätta övervakningen måste kommunikationsinfrastrukturens övervakningsverktyg kunna integreras med motsvarande verktyg hos den organisation som ansvarar för driftsledningen av SIS II-centralen.

6. **Bastjänster**

Utöver de specialiserade nät- och säkerhetstjänsterna måste kommunikationsinfrastrukturen också innehålla bastjänster.

De specialiserade tjänsterna måste av redundansskäl finnas i båda centralenheterna.

Följande tillvalda optiska bastjänster måste finnas i kommunikationsinfrastrukturen:

| Tjänst | Anmärkning |
|---|---|
| DNS | Reservomkoppling från CU till BCU som sker vid nätfel baseras i nuläget på byte av IP-adress inom den allmänna (generiska) DNS-servern. |
| E-postöverföring | Användning av en allmän (generisk) e-postöverföring kan vara praktisk för standardisering av e-postinstallationen för de olika medlemsstaterna. Till skillnad från en speciellt avdelad e-postserver binder en allmän e-postöverföring inte upp nätresurser från CU eller BCU.<br>E-post som sänds med en allmän e-postöverföring måste fortfarande överensstämma med sin säkerhetsmall (*security template*). |
| NTP | Kan användas för att synkronisera klockorna i nätutrustningen. |

7. **Tillgänglighet**

Oberoende av nätets tillgänglighet måste CS-SIS samt LNI och BLNI ha en tillgänglighet på 99,99 % mätt över 28 dagar.

Kommunikationsinfrastrukturens tillgänglighet måste vara 99,99 %.

8. **Säkerhetstjänster**

8.1 *Nätkryptering*

SIS II-centralen tillåter inte att data med höga eller mycket höga krav på dataskydd överförs utanför LAN utan kryptering. Det bör ordnas så att nätoperatören inte på något sätt har tillträde till operativa data i SIS II, och inte heller till datautbyte via Sirene-systemet.

För att hålla god säkerhet måste kommunikationsinfrastrukturen medge hantering av certifikat och nycklar. Det måste vara möjligt att fjärradministrera och fjärrövervaka krypteringsboxarna. Krypteringsalgoritmerna måste uppfylla minst följande krav:

— För symmetriska krypteringsalgoritmer:

  • 3DES (128 bitar) eller bättre.

  • Nyckelgenereringen måste baseras på slumpvärden som vid angrepp inte medger krympning av nyckelutrymmet (key space reduction).

  • Krypteringsnycklar eller information som kan användas för att härleda nycklarna måste alltid skyddas under lagring.

— För asymmetriska krypteringsalgoritmer:

  • 1 024 bitars RSA-kryptering eller bättre.

  • Nyckelgenereringen måste baseras på slumptal som vid angrepp inte medger krympning av nyckellängden.

Protokollet *Encapsulated Security Payload* (ESP, RFC2406) skall användas i tunnelmod. Payload-headern och den ursprungliga IP-headern skall krypteras.

För utbyte av sessionsnycklar skall protokollet *Internet Key Exchange* (IKE) användas.

IKE-nycklar får vara giltiga högst en dag, och sessionsnycklar högst en timme.

8.2 *Andra säkerhetsåtgärder*

Förutom att skydda anslutningspunkterna till SIS II måste kommunikationsinfrastrukturen skydda de tillvalda bastjänsterna. För dessa tjänster bör skyddsåtgärder vidtas som motsvarar dem i CS-SIS. Alla bastjänster måste därför som minimum ha en brandvägg, virusskydd och ett system för detektering av intrång. Dessutom bör utrustningen för bastjänsterna och dess skyddsåtgärder stå under kontinuerlig säkerhetsövervakning (loggning och uppföljning).

För att hålla god säkerhet måste den organisation som ansvarar för driftsledningen av SIS II-centralen ha information om alla säkerhetsincidenter som inträffar i kommunikationsinfrastrukturen. Infrastrukturen måste därför medge att alla viktigare säkerhetsincidenter utan dröjsmål anmäls till nämnda organisation. Alla sådana incidenter måste redovisas regelmässigt, t.ex. månadsvis och vid speciella behov.

9. **Helpdesk och support**

Den som sköter driften av kommunikationsinfrastrukturen måste tillhandahålla en helpdesk som samverkar med den organisation som ansvarar för driftsledningen av SIS II-centralen.

10. **Samverkan med andra system**

Kommunikationsinfrastrukturen måste hindra information från att gå utanför tilldelade kommunikationskanaler. För de tekniska lösningarna innebär det att

— allt obehörigt eller okontrollerat tillträde till andra nät är strängt förbjudet, inklusive anslutning till internet,

— dataläckage till andra system i nätet inte får inträffa. Det innebär t.ex. att sammankoppling av olika IP-VPN-nät inte är tillåten.

Förutom ovannämnda tekniska begränsningar som skyddet av informationsflödet leder till har skyddet också betydelse för kommunikationsinfrastrukturens helpdesk. Den får inte delge information om SIS II-centralen till någon annan än den som ansvarar för driftsledningen av centralen.