

II

(Az EK-Szerződés/Euratom-Szerződés alapján elfogadott jogi aktusok, amelyek közzététele nem kötelező)

HATÁROZATOK

BIZOTTSÁG

A BIZOTTSÁG HATÁROZATA

(2007. március 16.)

a Schengeni Információs Rendszer második generációjára vonatkozó hálózati követelmények (1. pillér) megállapításáról

(az értesítés a C(2007) 845. számú dokumentummal történt)

(Csak a bolgár, cseh, holland, német, észt, finn, görög, francia, magyar, olasz, lett, litván, máltai, lengyel, portugál, román, szlovák, szlovén, spanyol és svéd nyelvű szöveg hiteles)

(2007/170/EK)

AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA,

tekintettel az Európai Közösséget létrehozó szerződésre,

tekintettel a Schengeni Információs Rendszer második generációjának (SIS II) kifejlesztéséről szóló, 2001. december 6-i 2424/2001/EK tanácsi rendeletre ⁽¹⁾ és különösen annak (4) cikke a) pontjára,

mivel:

- (1) A SIS II kifejlesztéséhez meg kell határozni a kommunikációs hálózatra és annak elemeire vonatkozó műszaki előírásokat, valamint a speciális hálózati követelményeket.
- (2) Megfelelő rendelkezéseket kell létrehozni a Bizottság és a tagállamok között, különösen a tagállamokban lévő egységes nemzeti interfész elemei tekintetében.
- (3) Ez a határozat nem sérti a Bizottság egyéb, a SIS II kifejlesztéséhez kapcsolódó, különösen a biztonsági követelmények kialakításáról szóló határozatainak jövőbeni elfogadását.
- (4) A SIS II kifejlesztéséről a 2424/2001/EK rendelet és a 2001/886/IB tanácsi határozat ⁽²⁾ is rendelkezik. Annak érdekében, hogy a SIS II kifejlesztését szabályozó végre-

hajtási folyamat teljes egészében egységes legyen, e határozat rendelkezéseinek tükrözniük kell a Schengeni Információs Rendszer második generációjára (SIS II) vonatkozó hálózati követelmények megállapításáról szóló bizottsági határozat azon rendelkezéseit, amelyek a 2001/886/IB határozat alkalmazásában kerülnek elfogadásra.

- (5) Összhangban a Nagy-Britannia és Észak-Írország Egyesült Királyságának a schengeni vívmányok egyes rendelkezéseinek alkalmazásában való részvételére vonatkozó kéréséről szóló, 2000. május 29-i 2000/365/EK tanácsi határozattal ⁽³⁾, az Egyesült Királyság nem vett részt a 2424/2001/EK rendelet elfogadásában, így rá nézve az jogilag nem kötelező érvényű és nem alkalmazandó, mivel a rendelet a schengeni vívmányok rendelkezéseinek továbbfejlesztését jelenti. Az Egyesült Királyság ebből következően nem címzettje ezen határozatnak.
- (6) Összhangban Írországnak a schengeni vívmányok egyes rendelkezéseinek alkalmazásában való részvételére vonatkozó kéréséről szóló, 2002. február 28-i 2002/192/EK tanácsi határozattal ⁽⁴⁾, Írország nem vett részt a 2424/2001/EK rendelet elfogadásában, így rá nézve az jogilag nem kötelező érvényű és nem alkalmazandó, mivel a rendelet a schengeni vívmányok rendelkezéseinek továbbfejlesztését jelenti. Írország ebből következően nem címzettje ezen határozatnak.

⁽¹⁾ HL L 328., 2001.12.13., 4. o. Az 1988/2006/EK rendelettel (HL L 411., 2006.12.30., 1. o.) módosított rendelet.

⁽²⁾ HL L 328., 2001.12.13., 1. o.

⁽³⁾ HL L 131., 2000.6.1., 43. o. A 2004/926/EK határozattal (HL L 395., 2004.12.31., 70. o.) módosított határozat.

⁽⁴⁾ HL L 64., 2002.3.7., 20. o.

- (7) Az Európai Unióról szóló szerződéshez és az Európai Közösséget létrehozó szerződéshez csatolt, Dánia álláspontjáról szóló jegyzőkönyv 5. cikkének megfelelően Dánia úgy határozott, hogy a 2424/2001/EK tanácsi rendeletet végrehajtja a dán jogon keresztül. A 2424/2001/EK rendelet ennek megfelelően a nemzetközi jog szerint kötelező erejű Dániára nézve.
- (8) Izland és Norvégia tekintetében a 2424/2001/EK rendelet, valamint a 2001/886/IB határozat az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság között létrejött, e két államnak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodás⁽¹⁾ értelmében vett schengeni vívmányok azon rendelkezéseinek továbbfejlesztését jelentik, amelyek az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság között, e két államnak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról kötött megállapodás alkalmazását szolgáló egyes szabályokról szóló, 1999. május 17-i 1999/437/EK tanácsi határozat⁽²⁾ 1. cikkének B. pontjában említett területhez tartoznak.
- (9) Svájc tekintetében a 2424/2001/EK rendelet, valamint a 2001/886/IB határozat az Európai Unió, az Európai Közösség és a Svájci Államszövetség között létrejött, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról aláírt megállapodás értelmében vett schengeni vívmányok azon rendelkezéseinek továbbfejlesztése, amelyek az említett megállapodásnak az Európai Közösség nevében történő aláírásáról, valamint egyes rendelkezések ideiglenes alkalmazásáról szóló tanácsi határozat 4. cikkének (1) bekezdésében említett területre tartoznak.
- (10) E határozat a csatlakozási okmány 3. cikkének (1) bekezdése értelmében a schengeni vívmányokon alapuló, illetve azokkal egyéb módon összefüggő jogi aktus.
- (11) Az e határozatban foglalt intézkedések összhangban vannak a 2424/2001/EK rendelet 6. cikkének (1) bekezdése által létrehozott bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A SIS II kommunikációs infrastruktúrája fizikai architektúrájának megtervezéséhez kapcsolódó műszaki előírásokat e határozat melléklete határozza meg.

2. cikk

E határozat címzettjei a Belga Királyság, a Bolgár Köztársaság, Románia, a Cseh Köztársaság, a Németországi Szövetségi Köztársaság, az Észt Köztársaság, a Görög Köztársaság, a Spanyol Királyság, a Francia Köztársaság, az Olasz Köztársaság, a Ciprusi Köztársaság, a Lett Köztársaság, a Litván Köztársaság, a Luxemburgi Nagyhercegség, a Magyar Köztársaság, a Máltai Köztársaság, a Holland Királyság, az Osztrák Köztársaság, a Lengyel Köztársaság, a Portugál Köztársaság, a Szlovén Köztársaság, a Szlovák Köztársaság, a Finn Köztársaság, valamint a Svéd Királyság.

Kelt Brüsszelben, 2007. március 16-án.

a Bizottság részéről
Franco FRATTINI
alelnök

⁽¹⁾ HL L 176., 1999.7.10., 36. o.

⁽²⁾ HL L 176., 1999.7.10., 31. o.

MELLÉKLET

TARTALOMJEGYZÉK

1.	Bevezetés	23
1.1.	Mozaikszavak és rövidítések	23
2.	Általános áttekintés	24
3.	Földrajzi kiterjedés	24
4.	Hálózati szolgáltatások	25
4.1.	Hálózati elrendezés	25
4.2.	A CS-SIS fő- és tartalékpéldánya közötti kapcsolat típusa	25
4.3.	Sávszélesség	25
4.4.	Szolgáltatási kategóriák	25
4.5.	Támogatott protokollok	26
4.6.	Műszaki előírások	26
4.6.1.	IP-címzés	26
4.6.2.	Az IPv6 támogatása	26
4.6.3.	Statikus útvonalválasztás	26
4.6.4.	Fenntartott adatáramlási sebesség	26
4.6.5.	Egyéb előírások	26
4.7.	Rugalmasság	26
5.	Felügyelet	27
6.	Általános szolgáltatások	27
7.	Rendelkezésre állás	27
8.	Biztonságvédelmi szolgáltatások	27
8.1.	A hálózat titkosítása	27
8.2.	Egyéb biztonsági paraméterek	28
9.	Háttértámogatás	28
10.	Kommunikáció más rendszerekkel	28

1. Bevezetés

E dokumentum ismerteti a kommunikációs hálózat kialakítását, annak alkotóelemeit, valamint az egyedi hálózati követelményeket.

1.1. Mozaikszavak és rövidítések

Az alábbi szakasz a dokumentum további részében használt rövidítéseket ismerteti.

Mozaikszavak és rövidítések	Magyarázat
BLNI	Tartalék helyi nemzeti interfész (Backup Local National Interface)
CEP	Központi végpont (Central End Point)
CNI	Központi nemzeti interfész (Central National Interface)
CS	Központi rendszer (Central System)
CS-SIS	A SIS II adatbázist tartalmazó műszaki támogató funkció
DNS	Tartománynév-kiszolgáló (Domain Name Server)
FCIP	IP-alapú üvegszál hálózat (Fibre Channel over IP)
FTP	Fájltviteli protokoll (File Transport Protocol)
HTTP	Hiperszöveg-átviteli protokoll (Hyper Text Transfer Protocol)
IP	Internetprotokoll
LAN	Helyi hálózat (Local Area Network)
LNI	Helyi nemzeti interfész (Local National Interface)
Mbps	Megabit/másodperc
MDC	Fejlesztési fővállalkozó
N.SIS II	Az egyes tagállamokban található nemzeti szakasz
NI-SIS	Egységes nemzeti interfész
NTP	Hálózati idő protokoll (Network Time Protocol)
SAN	Adattároló hálózat (Storage Area Network)
SDH	Szinkron digitális hierarchia (Synchronous Digital Hierarchy)
SIS II	A Schengeni Információs Rendszer második generációja
SMTP	Egyszerű levéltovábbítási protokoll (Simple Mail Transport Protocol)
SNMP	Egyszerű hálózatkezelő protokoll (Simple Network Management Protocol)
s-TESTA	A közigazgatási szervek közötti biztonságos transzeurópai tematikai szolgáltatások, az IDABC programba (páneurópai e-kormányzati szolgáltatások közigazgatási szervek, üzleti vállalkozások és polgárok részére történő interoperábilis nyújtása, a 2004. április 21-i 2004/387/EK európai parlamenti és tanácsi határozat) tartozó intézkedés
TCP	Átvitelvezérlő protokoll (Transmission Control Protocol)
VIS	Vízuminformációs rendszer (Visa Information System)
VPN	Virtuális magánhálózat (Virtual Private Network)
WAN	Nagy kiterjedésű hálózat (Wide Area Network)

2. Általános áttekintés

A SIS II a következőkből áll:

- a központi rendszer (központi SIS II), amely a következőkből áll:
 - a SIS II adatbázist tartalmazó műszaki támogató funkció (CS-SIS). A CS-SIS fő része látja el a műszaki felügyeletet és adminisztrációt, míg a tartalék CS-SIS rendszerhiba esetén képes biztosítani a CS-SIS fő részének összes funkcióját,
 - egy egységes nemzeti interfész (NI-SIS),
- nemzeti szakasz (N.SIS II) minden egyes tagállamban, amely a központi SIS II-vel kommunikáló nemzeti adatrendszerekből áll. Az N.SIS II a SIS II adatbázisának teljes vagy részleges másolatából álló adatfájlt (nemzeti másolat) tartalmazhat,
- a CS-SIS és az NI-SIS közötti kommunikációs infrastruktúra (kommunikációs infrastruktúra), amely a SIS II adatok, valamint a SIRENE irodák közötti adatcsere céljára rendelt kódolt virtuális hálózatot képez.

Az NI-SIS a következőkből áll:

- minden tagállamban egy helyi nemzeti interfész (LNI), amely fizikailag összeköti a tagállamot a biztonságos kommunikációs hálózattal és tartalmazza a SIS II és a SIRENE forgalma számára fenntartott titkosítási eszközöket. Az LNI a tagállamok telephelyén helyezkedik el,
- nem kötelező tartalék helyi nemzeti interfész (BLNI), amely pontosan ugyanazzal a tartalommal és funkcióval rendelkezik, mint az LNI.

Az LNI és a BLNI kizárólag a SIS II rendszer és a SIRENE adatcseréire használható. Az LNI és a BLNI konkrét konfigurációját az egyes tagállamokkal együtt kell meghatározni és arról megállapodni annak érdekében, hogy tekintetbe vegyék a biztonsági követelményeket, a berendezés fizikai helyét és az üzembe helyezés feltételeit, beleértve a hálózati szolgáltató által biztosított szolgáltatásokat, azaz a fizikai s-TESTA kapcsolat tartalmazhat számos VPN alagutat más rendszerekhez, mint például a VIS és az Eurodac,

- egy központi nemzeti interfész (a továbbiakban: „CNI”), amely olyan alkalmazás, amely hozzáférést biztosít a CS-SIS-hez. Minden tagállamnak külön logikai hozzáférési pontja van a CNI-hez egy központi tűzfalon keresztül.

A CS-SIS és a NI-SIS közötti kommunikációs infrastruktúra a következőkből áll:

- a közigazgatási szervek közötti biztonságos transzeurópai tematikai szolgáltatások (a továbbiakban: s-TESTA) hálózata, amely a SIS II adatok, valamint a SIRENE adatforgalma számára titkosított virtuális magánhálózatot képez.

3. Földrajzi kiterjedés

A kommunikációs infrastruktúrának képesnek kell lennie az előírt szolgáltatások biztosítására és lefedésére minden tagállam számára.

Az összes EU-tagállam (Belgium, Franciaország, Németország, Luxemburg, Hollandia, Olaszország, Portugália, Spanyolország, Görögország, Ausztria, Dánia, Finnország, Svédország, Ciprus, Cseh Köztársaság, Észtország, Magyarország, Lettország, Litvánia, Málta, Lengyelország, Szlovákia, Szlovénia, az Egyesült Királyság és Írország), valamint Norvégia, Izland, Svájc.

Ezenkívül a most csatlakozott országok (Bulgária és Románia) lefedettségéről is gondoskodni kell.

Végül a kommunikációs infrastruktúrának alkalmasnak kell lennie arra, hogy kiterjeszhető legyen bármely más, a központi SIS II-höz csatlakozó országra vagy szervezetre (pl. Europol, Eurojust).

4. Hálózati szolgáltatások

Egy protokoll vagy architektúra említését úgy kell értelmezni, hogy egyenértékű jövőbeni technológiák, protokollok és architektúrák szintén elfogadhatók.

4.1. Hálózati elrendezés

A SIS II architektúrája központosított szolgáltatásokat alkalmaz, amelyek hozzáférhetőek a különböző tagállamokból. A rugalmasság céljából ezeket a központosított szolgáltatásokat megkettőzték, konkrétan a CS-SIS-t és a CU-t a franciaországi Strasbourgba, míg a tartalék CS-SIS-t és a tartalék CU-t az ausztriai St Johann im Pongauba telepítették.

A központi egységek fő- és tartalékrendszereinek elérhetőnek kell lenniük a különböző tagállamokból. A részt vevő országok többszörös hálózati hozzáférési pontokkal rendelkezhetnek, egy LNI-vel és egy BLNI-vel, amely összekapcsolja a nemzeti rendszert a központi szolgáltatásokkal.

A központi szolgálatokkal való fő összeköttetésen kívül a kommunikációs infrastruktúrának támogatnia kell a kétoldalú kiegészítő információcserét a különböző tagállamok SIRENE irodái között.

4.2. A CS-SIS fő- és tartalékpéldánya közötti kapcsolat típusa

A CS-SIS fő- és tartalékpéldányának összekapcsolásához szükséges kapcsolat típusa SDH gyűrű vagy egy azzal egyenértékű kapcsolattípus, ami azt jelenti, hogy nyitva kell állnia az új, jövőbeni architektúrák és technológiák számára is. Az SDH infrastruktúrát arra használják fel, hogy mindkét központi egység helyi hálózatát egyetlen egységes helyi hálózattá kapcsolják össze. Ezt a LAN-t a CU és a BCU folyamatos szinkronizálására használják fel.

4.3. Sáv szélesség

A kommunikációs infrastruktúra alapvetően fontos követelménye a sáv szélesség nagysága, amelyet a különböző összekapcsolt területeknek biztosíthat és az a képessége, hogy ezt a sáv szélességet a gerinchálózaton belül támogassa.

Az LNI-hez és a nem kötelező BLNI-hez szükséges sáv szélesség minden tagállam számára más lesz, főként a nemzeti másolatok, a központi keresés és a biometrikus információcsere használatának választásától függően.

Az, hogy a kommunikációs infrastruktúra ténylegesen milyen méretek nyújtása mellett dönt, lényegtelen mindaddig, amíg megfelel minden tagállam minimális szükségletének.

Minden egyes fent említett telephelytípus nagy mennyiségű adatot (alfanumerikus, biometrikus adatok és teljes dokumentumok) továbbíthat mindkét irányba. Ezért a kommunikációs infrastruktúrának megfelelő minimális garantált feltöltési és letöltési sebességet kell biztosítania minden egyes kapcsolathoz.

A kommunikációs infrastruktúrának 2 Mbps (megabit/másodperc) és 155 Mbps (megabit/másodperc) közötti vagy annál nagyobb méretű kapcsolatot kell biztosítania. A hálózatnak megfelelő minimális garantált feltöltési és letöltési sebességet kell biztosítania minden egyes csatlakozáshoz, és sebességénél fogva támogatnia kell a hálózati hozzáférési pontok sáv szélességének teljes nagyságát.

4.4. Szolgáltatási kategóriák

A központi SIS II támogatja a lekérdezések/figyelmeztetések rangsorolásának képességét. Származtatott követelményként a kommunikációs infrastruktúra a forgalom rangsorolásának lehetőségét is támogatni fogja.

A hálózati rangsorolási paramétereket a tervek szerint a központi SIS II állapítja meg minden olyan csomagra, amelyre szükséges. Az alkalmazott módszer a súlyozott, egyenlő esélyű sorba állítás. Ez feltételezi, hogy a kommunikációs infrastruktúra képes átvinni a forráshálózaton lévő adatcsomagokhoz hozzárendelt rangsorolást és a csomagokat ennek megfelelően kezelni saját gerinchálózatán belül. Továbbá a kommunikációs infrastruktúrának a távoli telephelyen azokat a kiindulási csomagokat kell szolgáltatnia, amelyek a forrás LAN-ban megállapított rangsorolást tartalmazzák.

4.5. Támogatott protokollok

A központi SIS II számos hálózati kommunikációs protokollt használ majd. A kommunikációs infrastruktúrának a hálózati kommunikációs protokollok széles skáláját kell támogatnia. A támogatandó szabvány protokollok a HTTP, FTP, NTP, SMTP, SNMP és a DNS.

A szabványos protokollokon kívül a kommunikációs infrastruktúrának különböző alagútprotokollok, a SAN replikációs protokollok és a szabadalmazott BEA WebLogic Java-to-Java kapcsolati protokolljainak kezelésére is alkalmasnak kell lennie. A titkosított forgalomnak a célállomáshoz történő továbbításához alagútprotokollokat használnak fel, mint például a biztonságos IP-alagút üzemmódban.

4.6. Műszaki előírások

4.6.1. IP-címzés

A kommunikációs infrastruktúrának egy sor foglalt IP-címmel kell rendelkeznie, amelyet csak az adott hálózatban lehet felhasználni. A foglalt IP-címtartományon belül a központi SIS II egy olyan dedikált IP-címcsoportot fog használni, amelyet sehol máshol nem alkalmaznak.

4.6.2. Az IPv6 támogatása

A tagállamok helyi hálózatában alkalmazott protokoll feltehetően a TCP/IP lesz. Néhány telephely azonban a 4. verzió, míg mások a 6. verzió alapulnak majd. A hálózati hozzáférési pontoknak lehetőséget kell nyújtaniuk arra, hogy átjáróként szolgáljanak, és alkalmasnak kell lenniük arra, hogy a SIS II-ben és az N.SIS II-ben egyaránt használt hálózati protokolloktól függetlenül működjenek.

4.6.3. Statikus útvonalválasztás

A CU és a BCU használhat egyetlen, azonos IP-címet a tagállamokkal való kommunikációhoz. Ezért a kommunikációs infrastruktúrának támogatnia kell a statikus útvonalválasztást.

4.6.4. Fenntartott adatáramlási sebesség

Mindaddig, amíg a CU vagy a BCU kapcsolat terhelése 90 % alatt van, az adott tagállamnak képesnek kell lennie arra, hogy folyamatosan fenntartsa meghatározott sávzélessége 100 %-át.

4.6.5. Egyéb előírások

A CS-SIS támogatásához a kommunikációs infrastruktúrának legalább a minimális műszaki előírásoknak meg kell felelnie:

Az átviteli késleltetés (a nagy forgalmú órákat is beleértve) a csomagok 95 %-ában 150 ms, vagy annál kevesebb kell hogy legyen, a csomagok 100 %-ában pedig kevesebb kell hogy legyen 200 ms-nál.

A csomagvesztés valószínűsége (a nagy forgalmú órákat is beleértve) a csomagok 95 %-ában 10^{-4} vagy annál kisebb, a csomagok 100 %-ában pedig 10^{-3} -nál kisebb kell, hogy legyen.

A fent említett előírásokat minden egyes hozzáférési pont esetében külön kell figyelembe venni.

A CU és a BCU közötti kapcsolat üzenetváltási késleltetése 60 ms vagy annál kevesebb lehet.

4.7. Rugalmasság

A CS-SIS megtervezésekor követelmény volt a magas szintű rendelkezésre állás. Emiatt a rendszer oly módon építette be a rugalmasságot az összetevők üzemzavarainak ellenszereként, hogy megkettőzte az összes berendezést.

A kommunikációs infrastruktúra összetevőinek az összetevők meghibásodásával szemben is rugalmasnak kell lenniük. A kommunikációs infrastruktúra szempontjából ez azt jelenti, hogy az alábbi összetevőknek kell rugalmasnak lenniük:

— gerinchálózat,

— útvonalválasztási készülékek,

- megjelenési pontok,
- helyihurok-kapcsolatok (beleértve a fizikailag fölösleges kábeleket),
- biztonsági berendezések (titkosítóberendezések, tűzfalak stb.),
- minden általános szolgáltatás (DNS, NTP stb.),
- LNI/BLNI.

Az átkapcsolásnak minden hálózati berendezés esetében kézi beavatkozás nélkül kell működnie.

5. Felügyelet

A felügyelet elősegítése érdekében a kommunikációs infrastruktúra felügyeleti eszközeinek alkalmasnak kell lenni arra, hogy integrálhatók legyenek a központi SIS II üzemeltetéséért felelős szervezet felügyeleti eszközeivel.

6. Általános szolgáltatások

A dedikált hálózati és biztonsági szolgáltatásokon kívül a kommunikációs infrastruktúrának általános szolgáltatásokat is kell nyújtania.

A dedikált szolgáltatásokat mindkét központi egységen belül meg kell valósítani a redundanciával összefüggő célok érdekében.

Az alábbi szabadon választható általános szolgáltatásoknak jelen kell lenniük a kommunikációs infrastruktúrában:

Szolgáltatás	További információk
DNS	Jelenleg a CU-ról a BCU-ra való vészhelyzeti átkapcsolási eljárás alapja hálózati hiba esetén az IP-címzések megváltoztatása az általános DNS szerveren belül.
E-mail továbbítás	Az általános e-mail relé használata hasznos lehet a különböző tagállamok e-mail telepítésének egységesítése céljából, és a dedikált szerverrel ellentétben semmit nem használ fel a CU/BCU hálózati forrásaiból. Az általános e-mail relét használó e-maileknek mindemellett meg kell felelniük biztonsági sablonjuknak.
NTP	Ez a szolgáltatás használható a hálózati berendezések óráinak összehangolásához.

7. Rendelkezésre állás

A CS-SIS-nek, valamint az LNI-nek és a BLNI-nek 99,99 %-os rendelkezésre állást kell tudni szolgáltatnia 28 napos folyamatos üzemelés mellett, kivéve a hálózati rendelkezésre állást.

A kommunikációs infrastruktúra rendelkezésre állásának aránya 99,99 %.

8. Biztonságvédelmi szolgáltatások

8.1. A hálózat titkosítása

A központi SIS II nem engedi, hogy magas, vagy igen magas védelmi követelményeket támasztó adatokat titkosítás nélkül a LAN-on kívülre továbbítsanak. Biztosítani kell, hogy a hálózati szolgáltató semmiképpen ne férjen hozzá a SIS II üzemeltetési adataihoz, illetve az azokhoz kapcsolódó SIRENE adatcserékhez.

A magas szintű biztonság fenntartása érdekében a kommunikációs infrastruktúrának lehetővé kell tennie a bizonyítványok/kulcsok kezelését. A titkosítási dobozok távoli rendszerfelügyeletét és távoli megfigyelését lehetségessé kell tenni. A titkosítási algoritmusoknak legalább az alábbi követelményeknek kell megfelelniük:

— Szimmetrikus titkosítási algoritmusok:

- 3DES (128 bits) vagy annál jobb.
- A kulcselőállításnak véletlenszerű értéken kell alapulnia, amely nem engedi a kulcsér csökkentését támadás alatt.
- A titkosítási kulcsok, illetve a kulcsok visszafejtéséhez használható információk a 002E tárolóban mindig védettek.

— Aszimmetrikus titkosítási algoritmusok:

- RSA (1 024 bites mód) vagy annál jobb.
- A kulcselőállításnak véletlenszerű értéken kell alapulnia, amely nem engedi a kulcsér csökkentését támadás alatt.

Beágyazott biztonsági adattartalom protokollt (ESP, RFC2406) kell használni, alagút üzemmódban. Az adattartalmat és az eredeti IP-fejléceket titkosítani kell.

A munkamenetkulcsok cseréléséhez az internetkulcs-cserélő protokollt (IKE) kell használni.

Az IKE kulcsok nem lehetnek érvényesek egy napnál tovább.

A munkamenetkulcsok nem lehetnek 1 óránál hosszabbak.

8.2. Egyéb biztonsági paraméterek

A SIS II hozzáférési pontok védelme mellett a kommunikációs infrastruktúrának a nem kötelező általános szolgáltatásokat is védenie kell. Ezeknek a szolgáltatásoknak a CS-SIS-éhez hasonló védelmi intézkedéseknek kell megfelelniük. Ezért minden általános szolgáltatást legalább tűzfalal, vírusirtóval és behatolásérzékelővel kell védeni. Továbbá az általános szolgáltatás eszközeit és védelmi intézkedéseit folyamatos biztonsági felügyelet alatt kell tartani (naplózás és nyomon követés).

A magas szintű biztonság fenntartása érdekében a központi SIS II üzemeltetéséért felelős szervezetnek tudomással kell bírnia bármilyen biztonsági problémáról, amely a kommunikációs infrastruktúrában jelentkezik. Ezért a kommunikációs infrastruktúrának lehetővé kell tennie, hogy a jelentősebb biztonsági problémákról késedelem nélkül jelentés készüljön a központi SIS II üzemeltetéséért felelős szervezet számára. Minden biztonsági problémáról rendszeresen, pl. havonta és eseti alapon beszámolót kell készíteni.

9. Háttértámogatás

A kommunikációs infrastruktúra szolgáltatójának támogatási szolgáltatást kell biztosítania, amely kapcsolatot tart a központi SIS II üzemeltetéséért felelős szervezettel.

10. Kommunikáció más rendszerekkel

A kommunikációs infrastruktúrának biztosítania kell, hogy az információ ne kerülhessen a kijelölt kommunikációs csatornákon kívülre. A technikai megvalósítás szempontjából ez azt jelenti, hogy:

- szigorúan tilos más hálózatokhoz való jogosulatlan és/vagy ellenőrizhetetlen hozzáférés. Ez magában foglalja az internetes kapcsolatokat,
- a hálózaton lévő más rendszerekbe nem szivároghat át adat; pl. nem megengedett a különböző IP VPN-ek (virtuális magánhálózatok) összekapcsolása.

A fent említett műszaki korlátozásokon kívül, amelyeket ez előídez, a kommunikációs infrastruktúra támogatási szolgáltatóra is hatással van. A támogatási szolgáltató nem adhat ki információt a központi SIS II-re vonatkozóan semmilyen más félnek, csakis a központi SIS II üzemeltetéséért felelős szervezetnek.