

II

(Akty prijaté podľa Zmluvy o ES/Zmluvy o Euratome, ktorých uverejnenie nie je povinné)

ROZHODNUTIA

KOMISIA

ROZHODNUTIE KOMISIE

zo 16. marca 2007,

ktorým sa ustanovujú sieťové požiadavky na Schengenský informačný systém II (1. pilier)

[oznámené pod číslom K(2007) 845]

(Iba bulharský, český, estónsky, fínsky, francúzsky, grécky, holandský, litovský, lotyšský, maďarský, maltský, nemecký, poľský, portugalský, rumunský, slovenský, slovinský, španielsky, švédsky a taliansky text je autentický)

(2007/170/ES)

KOMISIA EURÓPSKÝCH SPOLOČENSTIEV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva,

so zreteľom na nariadenie Rady (ES) č. 2424/2001 zo 6. decembra 2001 o vývoji druhej generácie Schengenského informačného systému (SIS II) ⁽¹⁾, a najmä na jeho článok 4 písm. a),

keďže:

- (1) V súvislosti s vývojom SIS II je potrebné stanoviť technické špecifikácie týkajúce sa komunikačnej siete a jej komponentov, ako aj špecifické sieťové požiadavky.
- (2) Medzi Komisiou a členskými štátmi by sa mali zaviesť primerané opatrenia, najmä pokiaľ ide o prvky jednotného národného rozhrania umiestneného v členských štátoch.
- (3) Týmto rozhodnutím nie je dotknuté prijímanie ďalších rozhodnutí Komisie v súvislosti s vývojom SIS II, najmä pokiaľ ide o vývoj bezpečnostných požiadaviek.

- (4) Vývoj SIS II sa riadi nariadením (ES) č. 2424/2001 a rozhodnutím Rady 2001/886/SVV ⁽²⁾. S cieľom zabezpečiť jednotný implementačný postup pri vývoji SIS II ako celku by ustanovenia tohto rozhodnutia mali premietnuť ustanovenia rozhodnutia Komisie, ktorým sa ustanovujú sieťové požiadavky na SIS II tak, aby bolo prijaté v súlade s uplatňovaním rozhodnutia 2001/886/SVV.

- (5) V súlade s rozhodnutím Rady 2000/365/ES z 29. mája 2000, ktoré sa týka požiadavky Spojeného kráľovstva Veľkej Británie a Severného Írska zúčastňovať sa na niektorých ustanoveniach schengenského *acquis* ⁽³⁾, sa Spojené kráľovstvo nezúčastnilo na prijatí nariadenia (ES) č. 2424/2001, nie je ním viazané a ani nepodlieha jeho uplatňovaniu, keďže toto nariadenie predstavuje vývoj ustanovení schengenského *acquis*. Toto rozhodnutie Komisie preto nie je určené Spojenému kráľovstvu.

- (6) V súlade s rozhodnutím Rady 2002/192/ES z 28. februára 2002 o požiadavke Írska zúčastňovať sa na niektorých ustanoveniach schengenského *acquis* ⁽⁴⁾ sa Írsko nezúčastnilo na prijatí nariadenia (ES) č. 2424/2001, nie je ním viazané a ani nepodlieha jeho uplatňovaniu, keďže toto nariadenie predstavuje vývoj ustanovení schengenského *acquis*. Toto rozhodnutie Komisie preto nie je určené Írsku.

⁽¹⁾ Ú. v. ES L 328, 13.12.2001, s. 4. Nariadenie zmenené a doplnené nariadením (ES) č. 1988/2006 (Ú. v. EÚ L 411, 30.12.2006, s. 1).

⁽²⁾ Ú. v. ES L 328, 13.12.2001, s. 1.

⁽³⁾ Ú. v. ES L 131, 1.6.2000, s. 43. Rozhodnutie zmenené a doplnené rozhodnutím 2004/926/ES (Ú. v. EÚ L 395, 31.12.2004, s. 70).

⁽⁴⁾ Ú. v. ES L 64, 7.3.2002, s. 20.

(²) Ú. v. ES L 176, 10.7.1999, s. 31.

PRÍLOHA

OBSAH

1.	Úvod	23
1.1.	Akronymy a skratky	23
2.	Všeobecný prehľad	24
3.	Geografické pokrytie	24
4.	Sieťové služby	25
4.1.	Štruktúra siete	25
4.2.	Typ spojenia medzi základným a záložným CS-SIS	25
4.3.	Šírka pásma	25
4.4.	Druhy služieb	25
4.5.	Podporované protokoly	26
4.6.	Technické špecifikácie	26
4.6.1.	Adresovanie IP	26
4.6.2.	Podpora IPv6	26
4.6.3.	Statické smerovanie	26
4.6.4.	Udržiavaná rýchlosť toku	26
4.6.5.	Ďalšie špecifikácie	26
4.7.	Odolnosť	26
5.	Monitorovanie	27
6.	Generické služby	27
7.	Dostupnosť	27
8.	Bezpečnostné služby	27
8.1.	Šifrovanie siete	27
8.2.	Ďalšie bezpečnostné prvky	28
9.	Helpdesk a štruktúra podpory	28
10.	Interakcia s inými systémami	28

1. Úvod

Tento dokument opisuje návrh komunikačnej siete, jej zahrnutých komponentov a špecifických sieťových požiadaviek.

1.1. Akronymy a skratky

Táto časť obsahuje akronymy použité v celom dokumente.

Akronymy a skratky	Vysvetlenie
BLNI	Záložné miestne národné rozhranie (Backup Local National Interface)
CEP	Centrálny koncový bod (Central End Point)
CNI	Centrálne národné rozhranie (Central National Interface)
CS	Centrálny systém (Central System)
CS-SIS	Technická podporná jednotka obsahujúca databázu SIS II
DNS	Server doménových mien (Domain Name Server)
FCIP	Optický kanál cez IP (Fibre Channel over IP)
FTP	Protokol prenosu súborov (File Transport Protocol)
HTTP	Hypertextový prenosový protokol (Hyper Text Transfer Protocol)
IP	Internetový protokol (Internet Protocol)
LAN	Miestna počítačová sieť (Local Area Network)
LNI	Miestne národné rozhranie (Local National Interface)
Mbit/s	Megabity za sekundu
MDC	Hlavný zmluvný vývojový dodávateľ (Main Developer Contractor)
N.SIS II	Národný úsek v každom členskom štáte
NI-SIS	Jednotné národné rozhranie
NTP	Časový protokol siete (Network Time Protocol)
SAN	Pamäťová sieť (Storage Area Network)
SDH	Synchrónna digitálna hierarchia (Synchronous Digital Hierarchy)
SIS II	Druhá generácia Schengenského informačného systému
SMTP	Jednoduchý protokol na prenos pošty (Simple Mail Transport Protocol)
SNMP	Jednoduchý protokol riadenia siete (Simple Network Management Protocol)
s-TESTA	Bezpečné transeurópske služby pre telematiku medzi správami – opatrenie programu IDABC (Vzájomná súčinnosť pri poskytovaní paneurópskych e-government služieb pre verejnú správu, podnikateľské subjekty a občanov, rozhodnutie Európskeho parlamentu a Rady 2004/387/ES z 21. apríla 2004)
TCP	Protokol riadenia prenosu (Transmission Control Protocol)
VIS	Vízový informačný systém (Visa Information System)
VPN	Virtuálna neverejná sieť (Virtual Private Network)
WAN	Rozsiahla počítačová sieť (Wide Area Network)

2. Všeobecný prehľad

SIS II pozostáva z:

- centrálneho systému (ďalej len „centrálny SIS II“), ktorý pozostáva z:
 - technickej podpornej jednotky (ďalej len „CS-SIS“), ktorá obsahuje databázu SIS II. Základná CS-SIS vykonáva technický dohľad a správu, pričom záložná CS-SIS dokáže zabezpečovať všetky funkcie základnej CS-SIS v prípade zlyhania tohto systému,
 - jednotného národného rozhrania (ďalej len „NI-SIS“),
- národného úseku (ďalej len „N.SIS II“) v každom členskom štáte, ktorý sa skladá z národných dátových systémov, ktoré komunikujú s centrálnym SIS II. N.SIS II môže obsahovať dátový súbor (ďalej len „národná kópia“) predstavujúci úplnú alebo čiastočnú kópiu databázy SIS II,
- komunikačnej infraštruktúry medzi CS-SIS a NI-SIS (ďalej len „komunikačná infraštruktúra“), ktorá zabezpečuje šifrovanú virtuálnu sieť pre údaje SIS II a výmenu údajov medzi úradmi SIRENE.

NI-SIS pozostáva z:

- miestneho národného rozhrania (ďalej len „LNI“) v každom členskom štáte, ktoré fyzicky pripája členské štáty k bezpečnej komunikačnej sieti a obsahuje šifrovacie zariadenia pre prevádzku SIS II a SIRENE. LNI je umiestnené na území členského štátu,
- voliteľného záložného miestneho národného rozhrania (ďalej len „BLNI“), ktoré má úplne rovnaký obsah a funkciu ako LNI.

Používanie LNI a BLNI je určené výhradne pre systém SIS II a výmenu SIRENE. Špecifická konfigurácia LNI a BLNI sa spresní a dohodne s každým jednotlivým členským štátom s cieľom zohľadniť bezpečnostné požiadavky, fyzické umiestnenie a podmienky inštalácie, vrátane poskytovania služieb poskytovateľom siete, čo znamená, že fyzické spojenie s-TESTA môže obsahovať niekoľko tunelov VPN pre iné systémy, napr. VIS a Eurodac,

- centrálneho národného rozhrania (ďalej len „CNI“), ktoré je aplikáciou umožňujúcou prístup do CS-SIS. Každý členský štát má samostatné logické prístupové body k CNI prostredníctvom centrálneho firewallu.

Komunikačná infraštruktúra medzi CS-SIS a NI-SIS pozostáva zo:

- siete pre bezpečné transeurópske služby pre telematiku medzi správami (ďalej len „s-TESTA“), ktorá zabezpečuje šifrovanú virtuálnu verejnú sieť pre údaje SIS II a prevádzku SIRENE.

3. Geografické pokrytie

Komunikačná infraštruktúra musí viesť zabezpečiť pokrytie a poskytovanie požadovaných služieb pre všetky členské štáty.

To znamená všetky členské štáty EÚ (Belgicko, Francúzsko, Nemecko, Luxembursko, Holandsko, Taliansko, Portugalsko, Španielsko, Grécko, Rakúsko, Dánsko, Fínsko, Švédsko, Cyprus, Česká republika, Estónsko, Maďarsko, Lotyšsko, Litva, Malta, Poľsko, Slovensko, Slovinsko, Spojené kráľovstvo a Írsko), ako aj Nórsko, Island a Švajčiarsko.

Okrem toho je potrebné zabezpečiť pokrytie aj pre prístupové krajiny Rumunsko a Bulharsko.

Nakoniec sa komunikačná infraštruktúra musí dať rozšíriť na akúkoľvek ďalšiu krajinu alebo subjekt, ktorý prístupí do centrálneho SIS II (napr. Europol, Eurojust).

4. Sieťové služby

Pri každom uvedenom protokole alebo architektúre sú prijateľné aj rovnaké budúce technológie, protokoly a architektúra.

4.1. Štruktúra siete

Architektúra SIS II využíva centralizované služby, ktoré sú prístupné z rôznych členských štátov. Pre potreby odolnosti sú tieto centralizované služby duplikované na dvoch rôznych miestach, konkrétne v Štrasburgu vo Francúzsku a v St. Johann im Pongau v Rakúsku, teda v CS-SIS, CU a záložnom CS-SIS, BCU.

Centrálne jednotky, hlavná a záložná, musia byť prístupné z rôznych členských štátov. Zúčastnené krajiny môžu mať viacero prístupových bodov siete, LNI a BLNI, ktoré slúžia na spojenie národného systému s centrálnymi službami.

Okrem hlavnej prepojitelnosti s centrálnymi službami musí komunikačná infraštruktúra podporovať aj dvojstrannú výmenu dodatočných informácií medzi úradmi SIRENE rôznych členských štátov.

4.2. Typ spojenia medzi základným a záložným CS-SIS

Požadovaným typom spojenia pre prepojitelnosť medzi základným a záložným CS-SIS musí byť SDH alebo rovnocenný kruh, t. j. musí byť otvorený aj pre nové budúce architektúry a technológie. Infraštruktúra SDH sa použije na rozšírenie miestnych sietí oboch centrálnych jednotiek s cieľom vytvorenia jednotnej konzistentnej LAN. Táto LAN sa následne využije na nepretržitú synchronizáciu CU a BCU.

4.3. Šírka pásma

Základnou požiadavkou komunikačnej infraštruktúry je veľkosť šírky pásma, ktorú môže poskytnúť rôznym prepojeným miestam, a jej schopnosť podporovať túto šírku pásma vnútri chrbtícovej siete.

Šírka pásma potrebná pre LNI a voliteľné BLNI sa bude v každom členskom štáte líšiť, a to najmä v závislosti od voľby používania národných kópií, centrálného vyhľadávania a výmeny biometrických údajov.

Konkrétna veľkosť, ktorú sa komunikačná infraštruktúra rozhodne ponúknuť, je irelevantná, pokiaľ spĺňa minimálne potreby každého členského štátu.

Každý z uvedených druhov miest môže prenášať obrovské množstvo údajov (alfanumerické, biometrické údaje, ako aj kompletne dokumenty) ľubovoľným smerom. Komunikačná infraštruktúra preto musí poskytovať dostatočne minimálne garantované rýchlosti vysielať a sťahovať pri každom spojení.

Komunikačná infraštruktúra musí ponúkať rýchlosť pripojenia od 2 do 155 Mbit/s alebo viac. Sieť musí poskytovať dostatočnú minimálnu garantovanú rýchlosť vysielať a sťahovať pri každom spojení a jej veľkosť musí umožňovať podporu celkovej veľkosti šírky pásma prístupových bodov siete.

4.4. Druhy služieb

Centrálny SIS II bude podporovať schopnosť prioritizácie dopytov/upozornení. V rámci odvodenej požiadavky bude komunikačná infraštruktúra podporovať aj možnosť prioritizácie prevádzky.

Predpokladá sa, že parametre sieťovej prioritizácie stanoví centrálny SIS II pre všetky pakety, pri ktorých je to potrebné. Použije sa pri tom vážené radenie (Weighted Fair Queuing), čo znamená, že komunikačná infraštruktúra musí byť schopná prevziať prioritizáciu zadanú dátovým paketom na zdrojovej LAN a primerane zoradiť pakety v rámci vlastnej chrbtícovej siete. Okrem toho na vzdialenom mieste musí komunikačná infraštruktúra doručiť pôvodné pakety obsahujúce rovnakú prioritizáciu, aká je nastavená v zdrojovej LAN.

4.5. Podporované protokoly

Centrálny SIS II bude využívať niekoľko sieťových komunikačných protokolov. Komunikačná infraštruktúra by mala podporovať rozsiahly súbor sieťových komunikačných protokolov. Medzi štandardnými protokolmi, ktoré majú byť podporované, sú HTTP, FTP, NTP, SMTP, SNMP a DNS.

Okrem štandardných protokolov musí byť komunikačná infraštruktúra schopná spracovať rôzne tunelovacie protokoly, replikačné protokoly SAN a protokoly spojenia Java-to-Java v rámci BEA WebLogic. Tunelovacie protokoly, ako napr. IPsec v tunelovom režime, sa použijú na prenos šifrovanej prevádzky na miesto určenia.

4.6. Technické špecifikácie

4.6.1. Adresovanie IP

Komunikačná infraštruktúra musí mať celý rad rezervovaných adries IP, ktoré možno použiť výlučne v rámci tejto siete. V rámci škály rezervovaných IP bude centrálny SIS II používať určený súbor adries IP, ktoré sa nebudú používať nikde inde.

4.6.2. Podpora IPv6

Možno predpokladať, že v miestnych sieťach členských štátov sa bude používať protokol TCP/IP. Niektoré miesta však budú vychádzať z verzie 4 a niektoré z verzie 6. Prístupové body siete musia ponúkať možnosť slúžiť ako sieťový priebeh a musia byť schopné fungovať nezávisle od sieťových protokolov používaných v centrálnom SIS II, ako aj v N.SIS II.

4.6.3. Statické smerovanie

Na komunikáciu s členskými štátmi môžu CU a BCU využívať jednu identickú adresu IP. Preto by komunikačná infraštruktúra mala podporovať statické smerovanie.

4.6.4. Udržiavaná rýchlosť toku

Len čo je rýchlosť zavedenia spojenia s CU alebo BCU menej ako 90 %, daný členský štát musí byť schopný nepretržite udržiavať 100 % vlastnej špecifikovanej šírky pásma.

4.6.5. Ďalšie špecifikácie

Na zabezpečenie podpory CS-SIS musí komunikačná infraštruktúra spĺňať aspoň minimálny súbor technických špecifikácií.

Oneskorenie trasy musí byť (vrátane hlavných prevádzkových hodín) maximálne 150 ms pri 95 % paketov a menej ako 200 ms pri 100 % paketov.

Pravdepodobnosť straty paketov musí byť (vrátane hlavných prevádzkových hodín) maximálne 10^{-4} pri 95 % paketov a menej ako 10^{-3} pri 100 % paketov.

Uvedené špecifikácie sa vzťahujú na každý prístupový bod samostatne.

Obojsmerné oneskorenie spojenia medzi CU a BCU môže byť maximálne 60 ms.

4.7. Odolnosť

Navrhnutý CS-SIS spĺňa požiadavku vysokej dostupnosti. Práve preto systém zahŕňa odolnosť proti zlyhaniu komponentov, a to na základe duplikovania všetkých zariadení.

Komponenty komunikačnej infraštruktúry musia byť odolné aj proti zlyhaniu komponentov. Pre komunikačnú infraštruktúru to znamená odolnosť nasledujúcich komponentov:

— chrbticovej siete,

— smerovacích zariadení,

- bodov prístupu,
- miestnych slučkových spojení (vrátane fyzických prebytočných káblov),
- bezpečnostných zariadení (šifrovacích zariadení, firewallov atď.),
- všetkých generických služieb (DNS, NTP atď.),
- LNI/BLNI.

Opravné mechanizmy (failover mechanisms) by sa mali vo všetkých sieťových zariadeniach spustiť bez manuálneho zásahu.

5. Monitorovanie

Na umožnenie monitorovania sa musia dať monitorovacie nástroje komunikačnej infraštruktúry začleniť do monitorovacích zariadení organizácie zodpovednej za prevádzkové riadenie centrálneho SIS II.

6. Generické služby

Okrem určených sieťových a bezpečnostných služieb musí komunikačná infraštruktúra ponúkať aj generické služby.

Určené služby sa musia pre nadbytočnosť implementovať v rámci oboch centrálnych jednotiek.

V komunikačnej infraštruktúre musia byť prítomné nasledujúce voliteľné generické služby:

Služba	Doplňujúce informácie
DNS	Súčasný opravný postup na prepnutie z CU na BCU v prípade sieťového zlyhania sa zakladá na zmene adresy IP v rámci servera generickej DNS.
Prenos e-mailov	Použitie generického prenosu e-mailov môže byť užitočné pre štandardizáciu e-mailového nastavenia pre rôzne členské štáty a na rozdiel od určeného servera nespotrebuje sieťové zdroje z CU/BCU. E-maily používajúce generický e-mailový prenos musia naďalej vyhovovať svojej bezpečnostnej predlohe.
NTP	Táto služba sa môže využiť na synchronizáciu hodín sieťových zariadení.

7. Dostupnosť

CS-SIS, LNI a BLNI musia byť dostupné na 99,99 % počas 28-dňového rolovacieho obdobia s výnimkou dostupnosti siete.

Dostupnosť komunikačnej infraštruktúry musí byť 99,99 %.

8. Bezpečnostné služby

8.1. Šifrovanie siete

Centrálny SIS II neumožňuje prenos údajov s vysokými alebo veľmi vysokými požiadavkami ochrany mimo LAN bez šifrovania. Malo by sa zabezpečiť, aby poskytovateľ siete nemal žiadnym spôsobom prístup k prevádzkovým údajom SIS II ani k príslušnej výmene SIRENE.

Na uchovanie vysokého stupňa bezpečnosti musí komunikačná infraštruktúra umožňovať riadenie certifikátov/kľúčov. Musí byť možná vzdialená správa a vzdialené monitorovanie šifrovacích okien. Šifrovacie algoritmy musia spĺňať nasledujúce minimálne požiadavky:

— symetrické šifrovacie algoritmy:

- 3DES (128 bitov) alebo viac,
- generácia kľúča musí byť založená na náhodnej hodnote, ktorá zabráni obmedzeniu priestoru kľúča v prípade útoku,
- šifrovacie kľúče alebo informácie, ktoré možno použiť na odvodenie kľúčov, majú zabezpečenú neustálu ochranu v pamäti,

— asymetrické šifrovacie algoritmy:

- RSA (1 024-bitový modul) alebo viac,
- generácia kľúča musí byť založená na náhodnej hodnote, ktorá zabráni obmedzeniu priestoru kľúča v prípade útoku.

Použije sa protokol zapuzdrených užitočných dát (ESP, RFC2406), a to v tunelovom režime. Používateľské dáta a pôvodné záhlavie IP budú šifrované.

Na výmenu relačných kľúčov sa použije protokol výmeny internetových kľúčov (IKE).

Kľúče IKE budú platné maximálne 1 deň.

Relačné kľúče budú platné maximálne 1 hodinu.

8.2. *Ďalšie bezpečnostné prvky*

Okrem ochrany prístupových bodov SIS II musí komunikačná infraštruktúra chrániť aj voliteľné generické služby. Tieto služby by mali spĺňať rovnaké ochranné opatrenia porovnateľné s opatreniami v prípade CS-SIS. Všetky generické služby preto musia byť chránené minimálne firewallom, antivírusovým softvérom a systémom na detekciu prienikov. Zariadenia generických služieb a ich ochranné opatrenia by navyše mali byť pod neustálym bezpečnostným dohľadom (registrácia a následné opatrenia).

Na udržanie vysokého stupňa bezpečnosti musí byť organizácia, ktorá je zodpovedná za prevádzkové riadenie centrálneho SIS II, oboznámená so všetkými bezpečnostnými incidentmi, ktoré v komunikačnej infraštruktúre nastanú. Preto musí komunikačná infraštruktúra umožniť, aby sa všetky veľké bezpečnostné incidenty hlásili bez akéhokoľvek omeškania príslušnej organizácii, ktorá je zodpovedná za prevádzkové riadenie centrálneho SIS II. Všetky bezpečnostné incidenty sa musia pravidelne vykazovať, napr. formou mesačných hlásení a *ad hoc* hlásení.

9. **Helpdesk a štruktúra podpory**

Poskytovateľ komunikačnej infraštruktúry musí zabezpečovať helpdesk, ktorý komunikuje s organizáciou zodpovednou za prevádzkové riadenie centrálneho SIS II.

10. **Interakcia s inými systémami**

Komunikačná infraštruktúra musí zabezpečiť, aby sa informácie nemohli dostať mimo pridelených komunikačných kanálov. Z hľadiska technickej implementácie to znamená, že:

- každý neoprávnený a/alebo nekontrolovaný prístup k iným sieťam je prísne zakázaný; platí to aj pre prepojitelnosť s internetom,
- nesmie dochádzať k úniku údajov do iných systémov v sieti, napr. nie je povolená prepojitelnosť s inými IP VPN.

Okrem uvedených technických obmedzení má vplyv aj na helpdesk komunikačnej infraštruktúry. Helpdesk nesmie poskytnúť žiadne informácie v súvislosti s centrálnym SIS II inému subjektu ako subjektu, ktorý je zodpovedný za prevádzkové riadenie centrálneho SIS II.
