II

(Актове, приети по силата на договорите ЕО/Евратом, чието публикуване не е задължително)

РЕШЕНИЯ

КОМИСИЯ

РЕШЕНИЕ НА КОМИСИЯТА

от 16 март 2007 година

относно определяне на мрежовите изисквания за Шенгенската информационна система II (1-ви стълб)

(нотифицирано под номер C(2007) 845)

(само текстовете на български, гръцки, естонски, испански, италиански, латвийски, литовски, малтийски, немски, нидерландски, полски, португалски, румънски, словашки, словенски, унгарски, фински, френски, чешки и шведски език са автентични)

(2007/170/ЕО)

КОМИСИЯТА НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската общност,

като взе предвид Решение (ЕО) № 2424/2001 на Съвета от 6 декември 2001 г. за разработване на второ поколение Шенгенска информационна система (ШИС II) ([1]), и по-специално член 4, буква а) от него,

като има предвид, че:

(1) За разработване на ШИС II е необходимо да се определят технически спецификации относно комуникационната мрежа, нейните компоненти и специфичните мрежови изисквания.

(2) Следва да се въведат подходящи процедури между Комисията и държавите-членки, по-специално по отношение на елементите на единния национален интерфейс в държавите-членки.

(3) Настоящото решение не засяга приемането в бъдеще на друго решение на Комисията, свързано с разработването на ШИС II, по-специално относно разработването на изискванията за сигурност.

(4) Регламент (ЕО) № 2424/2001 и Решение 2001/886/ПВР на Съвета ([2]) регулират разработването на ШИС II. За да се гарантира прилагане на един и същи процес на изпълнение за разработването на ШИС II като цяло, разпоредбите на настоящото решение следва да отразяват разпоредбите на решението на Комисията относно определяне на мрежовите изисквания за ШИС II, което трябва да бъде прието в съответствие с Решение 2001/886/ПВР.

(5) В съответствие с Решение 2000/365/ЕО на Съвета от 29 май 2000 г. относно искането на Обединеното кралство Великобритания и Северна Ирландия да участва в някои разпоредби от достиженията на правото от Шенген ([3]) Обединеното кралство не взе участие в приемането на Регламент (ЕО) № 2424/2001, не е обвързано с него и не е обект на прилагането му, тъй като той представлява разработване на разпоредби на достижението на правото от Шенген. Следователно Обединеното кралство не е адресат на настоящото решение на Комисията.

(6) В съответствие с Решение 2002/192/ЕО на Съвета от 28 февруари 2002 г. относно искането на Ирландия да участва в някои разпоредби от достиженията на правото от Шенген ([4]) Ирландия не взе участие в приемането на Регламент (ЕО) № 2424/2001, не е обвързана с него и не е обект на прилагането му, тъй като той представлява разработване на разпоредби на достижението на правото от Шенген. Следователно Ирландия не е адресат на настоящото решение на Комисията.

([1]) ОВ L 328, 13.12.2001 г., стр. 4. Регламент, изменен с Регламент (ЕО) № 1988/2006 (ОВ L 411, 30.12.2006 г., стр. 1).

([2]) ОВ L 328, 13.12.2001 г., стр. 1.

([3]) ОВ L 131, 1.6.2000 г., стр. 43. Решение, изменено с Решение 2004/926/ЕО (ЕО L 395, 31.12.2004 г., стр. 70).

([4]) ОВ L 64, 7.3.2002 г., стр. 20.

(7) Съгласно член 5 от Протокола за позицията на Дания, приложен към Договора за Европейския съюз и Договора за създаване на Европейската общност, Дания взе решение да приложи Регламент (ЕО) № 2424/2001 в датското законодателство. Поради това Регламент (ЕО) № 2424/2001 е обвързващ за Дания в международното законодателство.

(8) По отношение на Исландия и Норвегия Регламент (ЕО) № 2424/2001 и Решение 2001/883/ПВР представляват разработване на разпоредбите от достиженията на правото от Шенген по смисъла на споразумението, сключено от Съвета на Европейския съюз с Република Исландия и с Кралство Норвегия относно асоциирането на тези две държави с въвеждането, прилагането и развитието на достиженията на правото от Шенген [1], което попада в областта, посочена в член 1, буква Б от Решение 1999/437/ЕО на Съвета от 17 май 1999 година относно определени условия по прилагането на Споразумението между Европейския съюз и Република Исландия и Кралство Норвегия за асоцииране на тези две държави при изпълнението, прилагането и развитието на достиженията на правото от Шенген [2].

(9) По отношение на Швейцария Регламент (ЕО) № 2424/2001 и Решение 2001/886/ПВР представляват разработване на разпоредбите от достиженията на правото от Шенген по смисъла на споразумението, подписано между Европейския съюз, Европейската общност и Конфедерация Швейцария относно асоциирането на Конфедерация Швейцария с въвеждането, прилагането и развитието на достиженията на правото от Шенген, което попада в областта, посочена в член 4, параграф 1 от решението на Съвета за подписване от името на Европейската общност и за временно прилагане на някои разпоредби от това споразумение.

(10) Настоящото решение представлява акт, изграден на основата на достиженията на правото от Шенген или свързан по друг начин с тях по смисъла на член 3, параграф 1 от Акта за присъединяване.

(11) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, учреден с член 6, параграф 1 от Регламент (ЕО) № 2424/2001,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Техническите спецификации, свързани с конструирането на физическата архитектура на комуникационната инфраструктура на ШИС II, се определят в приложението.

Член 2

Адресати на настоящото решение са Кралство Белгия, Република България, Чешката република, Федерална република Германия, Република Естония, Република Гърция, Кралство Испания, Френската република, Италианската република, Република Кипър, Република Латвия, Република Литва, Великото херцогство Люксембург, Република Унгария, Република Малта, Кралство Нидерландия, Република Австрия, Република Полша, Португалската република, Румъния, Република Словения, Словашката република, Република Финландия и Кралство Швеция.

Съставено в Брюксел на 16 март 2007 година.

За Комисията

Franco FRATTINI

Заместник-председател

[1] ОВ L 176, 10.7.1999 г., стр. 36.
[2] ОВ L 176, 10.7.1999 г., стр. 31.

ПРИЛОЖЕНИЕ

СЪДЪРЖАНИЕ

1. **Въведение**

Настоящият документ описва конструирането на комуникационната мрежа, нейните компоненти и специфичните мрежови изисквания.

1.1. *Акроними и съкращения*

В този раздел са посочени акронимите, използвани в документа.

Акроними и съкращения	Обяснение
РЛНИ	Резервен локален национален интерфейс
CEP	Central End Point
ЦНИ	Централен национален интерфейс
ЦС	Централна система
ЦС-ШИС	Структура по техническо подпомагане, съдържаща базата данни на ШИС II
DNS	Domain Name Server
FCIP	Fibre Channel over IP
FTP	File Transport Protocol (протокол за обмен на файлове)
HTTP	Hyper Text Transfer Protocol (протокол за обмен на хипертекст)
IP	Internet Protocol (интернет протокол)
LAN	Local Area Network (локална мрежа)
ЛНИ	Локален национален интерфейс
Mbps	Megabits per second (мегабита в секунда)
ГИР	Главен изпълнител на разработването
Н.ШИС II	Националната част във всяка държава-членка
НИ-ШИС	Единен национален интерфейс
NTP	Network Time Protocol
SAN	Storage Area Network (мрежа за съхранение на данни)
SDH	Synchronous Digital Hierarchy (синхронна цифрова йерархия)
ШИС II	Шенгенска информационна система, второ поколение
SMTP	Simple Mail Transport Protocol (прост протокол за обмен на електронна поща)
SNMP	Simple Network Management Protocol (прост протокол за управление на мрежата)
s-TESTA	Secure Trans-European Services for Telematics between Administrations (защитени трансевропейски телематични услуги между администрациите) е мярка по програма IDABC (Interoperable delivery of pan-European eGovernment services to public administrations, business and citizens — оперативно съвместимо предоставяне на паневропейски услуги по електронно правителство за публичните администрации, фирмите и гражданите. Решение 2004/387/ЕО на Европейския парламент и на Съвета от 21 април 2004 г.).
TCP	Transmission Control Protocol (протокол за управление на обмена на информация)
ВИС	Визова информационна система
VPN	Virtual Private Network (виртуална частна мрежа)
WAN	Wide Area Network (глобална мрежа)

2. **Общ преглед**

ШИС II е съставена от:

— централна система (наричана по-нататък „централна ШИС II“), която се състои от:

• структура по техническо подпомагане (наричана по-нататък „ЦС-ШИС“), съдържаща базата данни на ШИС II. Главната ЦС-ШИС извършва технически надзор и управление, а резервна ЦС-ШИС е в състояние да осигури всички функции на главната ЦС-ШИС в случай на неизправност на тази система,

• единен национален интерфейс (наричан по-нататък „НИ-ШИС“);

— национална част (наричана по-нататък „Н.ШИС II“) във всяка държава-членка, състояща се от националните системи за данни, които са свързани с централната ШИС II. Н.ШИС II може да съдържа файл с данни (наричан по-нататък „национално копие“), който съдържа пълно или частично копие на базата данни на ШИС II;

— комуникационна инфраструктура между ЦС-ШИС и НИ-ШИС (наричана по-нататък „комуникационна инфраструктура“), която осигурява криптирана виртуална мрежа, предназначена за данни на ШИС II и обмена на данни между бюрата SIRENE.

НИ-ШИС се състои от:

— един локален национален интерфейс (наричан по-нататък „ЛНИ“) във всяка държава-членка, който е интерфейсът, свързващ физически държавата-членка със защитената комуникационна мрежа и съдържащ криптиращите устройства, предназначени за трафика на ШИС II и SIRENE. ЛНИ се намира в държавата-членка;

— незадължителен резервен локален национален интерфейс (наричан по-нататък „РЛНИ“), който има същото съдържание и функция като ЛНИ.

ЛНИ и РЛНИ се използват само от ШИС II и за обмен на информация със SIRENE. Специфичната конфигурация на ЛНИ и РЛНИ ще бъде уточнена и договорена с всяка отделна държава-членка, за да се вземат предвид изискванията за сигурност, физическото местоположение и условията на инсталиране, включително предоставянето на услуги от мрежовия доставчик, така че физическата връзка s-TESTA да съдържа няколко VPN тунела за други системи, например ВИС и Евродак;

— централен национален интерфейс (наричан по-нататък „ЦНИ“), който е приложение, осигуряващо защита на достъпа до ЦС-ШИС. Всяка държава-членка има отделни логически точки за достъп до ЦНИ през централна защитна стена (файъруол).

Комуникационната инфраструктура между ЦС-ШИС и НИ-ШИС се състои от:

— мрежата за защитени трансевропейски телематични услуги между администрациите (наричана по-нататък „s-TESTA“), която осигурява криптирана виртуална частна мрежа, предназначена за данни на ШИС II и трафика на SIRENE.

3. **Географско покритие**

Комуникационната инфраструктура трябва да може да обхваща и предоставя необходимите услуги на всички държави-членки:

Всички държави-членки на ЕС (Белгия, Франция, Германия, Люксембург, Нидерландия, Италия, Португалия, Испания, Гърция, Австрия, Дания, Финландия, Швеция, Кипър, Чешка република, Естония, Унгария, Латвия, Литва, Малта, Полша, Словакия, Словения, Обединено кралство и Ирландия), както и Норвегия, Исландия и Швейцария.

Освен това трябва да се осигури покритие на новоприсъединилите се страни Румъния и България.

И накрая, комуникационната инфраструктура трябва да позволява разширяването ѝ до всяка друга страна или субект, който има достъп до централната ШИС II (например. Европол, Евроюст).

4. **Мрежови услуги**

Когато е посочен даден протокол или архитектура, следва да се разбира, че еквивалентните бъдещи технологии, протоколи и архитектура също са допустими.

4.1. *Структура на мрежата*

Архитектурата на ШИС II използва централизирани услуги, достъпни от отделните държави-членки. С цел устойчивост на системата тези централизирани услуги са дублирани на две различни места, а именно Страсбург във Франция и Сен Йохан им Понгау в Австрия, където се намират съответно ЦС-ШИС (централно звено — ЦЗ) и резервната ЦС-ШИС (резервно централно звено — РЦЗ).

Централните звена, главно и резервно, трябва да бъдат достъпни от отделните държави-членки. Участващите страни могат да имат няколко точки за достъп до мрежата, ЛНИ и РЛНИ, за да свържат своите национални системи с централните услуги.

Освен главната връзка към централните услуги комуникационната инфраструктура трябва също да поддържа двустранен обмен на допълнителна информация между бюрата SIRENE на отделните държави-членки.

4.2. *Вид връзка между главната ЦС-ШИС и резервната ЦС-ШИС*

Необходимият тип връзка за свързване на главната ЦС-ШИС и резервната ЦС-ШИС трябва да бъде SDH ring или еквивалентна на нея, т.е. връзката да бъде възможна и в бъдеще с нови архитектури и технологии. Инфраструктурата SDH ще бъде използвана за разширяване на локалните мрежи на централните звена за създаване на непрекъсната единна LAN. Тази LAN ще се използва за постоянно синхронизиране между ЦЗ и РЦЗ.

4.3. *Честотна лента*

Важно изискване за комуникационната инфраструктура е широчината на честотната лента, която тази инфраструктура може да предостави на отделните свързани сайтове, и способността ѝ да поддържа тази честотна лента в нейната опорна мрежа.

Необходимата честотна лента за ЛНИ и незадължителния РЛНИ ще бъде различна за всяка държава-членка, като това ще зависи главно от избора за използване на национални копия, централно търсене и обмен на биометрични данни.

Реалната широчина на честотната лента, която комуникационната инфраструктура реши да предостави, е без значение, стига да отговаря на минималните нужди на всяка държава-членка.

Всеки един от посочените по-горе видове сайтове може да пренася значителен обем данни (буквено-цифрови, биометрични и цели документи) във всяка от двете посоки. Ето защо комуникационната инфраструктура трябва да осигурява достатъчна минимална гарантирана скорост за ъплоуд (качване на файлове) и даунлоуд (изтегляне на файлове) за всяка връзка.

Комуникационната инфраструктура трябва да предлага връзка от 2 Mbps до 155 Mbps или повече. Мрежата трябва да осигурява достатъчна минимална гарантирана скорост за ъплоуд и даунлоуд за всяка връзка и трябва да бъде в състояние да поддържа цялата честотна лента на точките за достъп до мрежата.

4.4. *Категории услуги*

Централната ШИС II ще може да обработва заявките/сигналите в зависимост от приоритета им. Вследствие на това комуникационната инфраструктура също ще може да поддържа управление на трафика в зависимост от приоритета.

Приема се, че параметрите за определяне на приоритети на мрежата трябва да се установят от централната ШИС II за всички пакети данни, които го изискват. Ще се използва механизмът Weighted Fair Queuing. Това предполага, че комуникационната инфраструктура трябва да може да приеме приоритета, зададен на пакетите данни в LAN източника, и да обработи пакетите спрямо този приоритет в своята опорна мрежа. Освен това комуникационната инфраструктура трябва да достави на отдалечения сайт началните пакети, които имат същия приоритет като зададения в LAN източника.

4.5. *Поддържани протоколи*

Централната ШИС II ще използва няколко мрежови протокола за комуникация. Комуникационната инфраструктура следва да поддържа широк спектър от мрежови протоколи за комуникация. Стандартните протоколи, които трябва да се поддържат, са HTTP, FTP, NTP, SMTP, SNMP и DNS.

Освен стандартните протоколи комуникационната инфраструктура трябва също да е в състояние да управлява различни тунелни протоколи, SAN replication протоколи и патентованите протоколи за Java-to-Java връзка на BEA WebLogic. Тунелните протоколи, например IPsec в тунелен режим, ще се използват за пренос на криптиран трафик до местоназначението му.

4.6. *Технически спецификации*

4.6.1. IP адресиране

Комуникационната инфраструктура трябва да разполага със серия запазени IP адреси, които могат да бъдат използвани единствено в тази мрежа. От тези запазени IP адреси централната ШИС II ще използва определен брой IP адреси, които ще бъдат използвани само в нея.

4.6.2. Поддържане на IPv6

Може да се приеме, че протоколът, използван в локалните мрежи на държавите-членки, ще бъде TCP/IP. Въпреки това някои сайтове ще бъдат базирани на версия 4, а други — на версия 6. Точките за достъп до мрежата трябва да могат да функционират като шлюз и да са в състояние да работят независимо от мрежовите протоколи, използвани в централната ШИС II, както и в Н.ШИС II.

4.6.3. Статично маршрутизиране

Централното и резервното централно звено могат да използват един и същ IP адрес за комуникацията си с държавите-членки. Поради това комуникационната инфраструктура следва да поддържа статично маршрутизиране.

4.6.4. Постоянен трансфер

При условие че натовареността на връзката на централното и резервното централно звено е по-малка от 90 %, дадена държава-членка трябва да може да поддържа без прекъсване 100 % от своята определена честотна лента.

4.6.5. Други спецификации

За да поддържа ЦС-ШИС, комуникационната инфраструктура трябва да отговаря поне на един минимален брой технически спецификации.

Времето за предаване (включително в натоварените часове) трябва да бъде по-малко или равно на 150 ms за 95 % от пакетите и по-малко от 200 ms за 100 % от пакетите.

Вероятността за загуба на пакети (включително в натоварените часове) трябва да бъде по-малка или равна на 10^{-4} за 95 % от пакетите и по-малка от 10^{-3} за 100 % от пакетите.

Горепосочените спецификации се разглеждат отделно за всяка точка за достъп.

За връзката между ЦЗ и РЦЗ времето за двупосочно предаване трябва да бъде по-малко или равно на 60 ms.

4.7. *Устойчивост*

ЦС-ШИС е проектирана да отговаря на изискването за висока степен на достъпност. Поради това системата се характеризира с цялостна устойчивост срещу неизправности в компонентите чрез дублиране на цялото оборудване.

Компонентите на комуникационната инфраструктура трябва също да бъдат устойчиви срещу повреда в някой от тях. За комуникационната инфраструктура това означава, че следните компоненти трябва да бъдат устойчиви:

— опорна мрежа,

— маршрутизиращи устройства,

— точки на присъствие,

— локални връзки (включително резервни кабели),

— устройства за сигурност (криптиращи устройства, защитни стени и др.),

— всички основни услуги (DNS, NTP и др.),

— ЛНИ/РЛНИ.

В цялото мрежово оборудване резервните механизми в случай на повреда следва да се включват без ръчна намеса.

5. **Мониторинг**

За улесняване на мониторинга средствата за мониторинг, с които комуникационната инфраструктура разполага, трябва да могат да се интегрират с тези на съоръженията за мониторинг на организацията, която отговаря за оперативното управление на централната ШИС II.

6. **Общи услуги**

Освен специалните мрежови услуги и услуги за сигурност комуникационната структура трябва също да осигурява общи услуги.

Специалните услуги трябва да се изпълняват и в двете централни звена с цел осигуряване на резерв.

Следните общи услуги по избор трябва да са налични в комуникационната инфраструктура:

Услуга	Допълнителна информация
DNS	Понастоящем процедурата в случай на повреда за превключване от ЦЗ към РЦЗ при неизправност на мрежата се основава на смяна на IP адреса в общия DNS сървър.
Препредаване на електронна поща	Използването на общ предавател на електронна поща може да е от полза за стандартизиране на инсталирането на електронна поща за отделните държави-членки и, за разлика от един специализиран сървър, той не използва мрежови ресурси от ЦЗ/РЦЗ. Електронните съобщения, минаващи през общ предавател, трябва все пак да отговарят на техния модел за сигурност.
NTP	Тази услуга може да бъде използвана за синхронизиране на часовниците на мрежовото оборудване.

7. **Достъпност**

ЦС-ШИС, ЛНИ и РЛНИ трябва да бъдат в състояние да осигурят 99,99 % достъп в продължение на 28 дни без прекъсване, с изключение на достъпа до мрежата.

Комуникационната инфраструктура трябва да бъде достъпна 99,99 %.

8. **Услуги за сигурност**

8.1. *Криптиране на мрежата*

Централната ШИС II не позволява данни с високи или много високи изисквания за сигурност да се предават извън LAN мрежата без криптиране. Следва да се гарантира, че мрежовият доставчик няма достъп до оперативните данни на ШИС II, както и до съответния обмен на данни SIRENE.

За поддържане на висока степен на сигурност комуникационната инфраструктура трябва да дава възможност за управление на сертификатите/ключовете. Трябва да има възможност за отдалечено администриране и отдалечен мониторинг на криптиращите кутии (encryption boxes). Криптографските алгоритми трябва да съответстват поне на следните изисквания:

— симетрични криптографски алгоритми:

• 3DES (128 bits) или по-добри;

• генерирането на ключ трябва да зависи от произволна стойност, която не позволява намаляване на ключовото пространство (key space) при атака;

• криптографските ключове или информация, която може да бъде използвана за получаване на ключовете, трябва винаги да бъдат защитени при съхраняването им;

— асиметрични криптографски алгоритми:

• RSA (1 024 битови модули) или по-добри;

• генерирането на ключ трябва да зависи от произволна стойност, която не позволява намаляване на ключовото пространство (key space) при атака.

Използва се протокол Encapsulated Security Payload (ESP, RFC2406). Той се използва в тунелен режим. Полезният товар (payload) и оригиналната заглавна част на IP пакета (IP header) се криптират.

За обмен на сесийни ключове се използва протокол Internet Key Exchange (IKE).

IKE ключовете са валидни не повече от един ден.

Валидността на сесийните ключове е не повече от един час.

8.2. *Други елементи за сигурност*

Освен защита на точките за достъп до ШИС II комуникационната инфраструктура трябва също да осигурява защита на общите услуги по избор. Тези услуги следва да отговарят на същите изисквания за защита, както тези в ЦС-ШИС. Ето защо всички общи услуги трябва най-малкото да бъдат защитени със защитна стена, антивирусна програма и система за засичане на непозволен достъп. Освен това следва да се извършва постоянно наблюдение за сигурност на устройствата за общи услуги и техните мерки за защита (включване на потребители и проследяване).

С цел поддържане на висока степен на сигурност организацията, която отговаря за оперативното управление на централната ШИС II, трябва да бъде уведомявана за всеки инцидент, свързан със сигурността, който възниква в комуникационната инфраструктура. Следователно комуникационната инфраструктура трябва да позволява незабавно докладване на инциденти, свързани със сигурността, на организацията, която отговаря за оперативното управление на централната ШИС II. Всички инциденти, свързани със сигурността, трябва да се докладват редовно, например месечни доклади и доклади ad hoc.

9. **Бюро за помощ и структура за поддръжка**

Доставчикът на комуникационната инфраструктура трябва да осигури бюро за помощ (helpdesk), което да взаимодейства с организацията, която отговаря за оперативното управление на централната ШИС II.

10. **Взаимодействие с други системи**

Комуникационната инфраструктура трябва да гарантира, че информацията не може да излиза извън предвидените комуникационни канали. По отношение на техническото осъществяване това предполага, че:

— абсолютно се забранява всеки неоторизиран и/или неконтролиран достъп до други мрежи. Това включва връзката с Интернет;

— не може да има изтичане на информация към други системи в мрежата; например не се разрешава взаимната връзка между различни IP VPN.

Освен произтичащите технически ограничения, посочени по-горе, това засяга и бюрото за помощ на комуникационната инфраструктура. Бюрото за помощ не може да предоставя никаква информация относно централната ШИС II на никоя страна, освен тази, която отговаря за оперативното управление на централната ШИС II.