ISSN 1830-3617

Официален вестник L 210

на Европейския съюз

Година 51

Издание на български език Законодателство 6 август 2008 г.

Съдържание

Цена: 18 EUR

BG

Актовете, чиито заглавия се отпечатват с нормален шрифт, са актове по текущо управление на селскостопанската политика и имат кратък срок на действие.

Заглавията на всички останали актове се отпечатват с получер шрифт и се предшестват от звездичка.

III

(Актове, приети по силата на Договора за ЕС)

АКТОВЕ, ПРИЕТИ ПО СИЛАТА НА ДЯЛ VI ОТ ДОГОВОРА ЗА ЕС

РЕШЕНИЕ 2008/615/ПВР НА СЪВЕТА

от 23 юни 2008 година

за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за Европейския съюз, и по-специално член 30, параграф 1, букви а) и б), член 31, параграф 1, буква а), член 32 и член 34, параграф 2, буква в) от него,

като взе предвид инициативата на Кралство Белгия, Република България, Федерална република Германия, Кралство Испания, Френската република, Великото херцогство Люксембург, Кралство Нидерландия, Република Австрия, Република Словения, Словашката република, Италианската република, Република Финландия, Португалската република, Румъния и Кралство Швеция,

като взе предвид становището на Европейския парламент [1],

като има предвид, че:

(1) След влизането в сила на Договора между Кралство Белгия, Федерална република Германия, Кралство Испания, Френската република, Великото херцогство Люксембург, Кралство Нидерландия и Република Австрия относно засилването на трансграничното сътрудничество, по-специално в борбата срещу тероризма, трансграничната престъпност и незаконната миграция (наричан по-долу „Договора от Прюм“), настоящата инициатива се представя, след консултации с Европейската комисия, в съответствие с разпоредбите на Договора за Европейския съюз, с цел включване на съдържанието на разпоредбите на Договора от Прюм в правната рамка на Европейския съюз.

(2) Заключенията от заседанието на Европейския съвет в Тампере през октомври 1999 г. потвърдиха необходимостта от подобряване на обмена на информация между компетентните органи на държавите-членки с цел разкриване и разследване на нарушения.

(3) В Програмата от Хага за укрепване на свободата, сигурността и правосъдието в Европейския съюз от ноември 2004 г. Европейският съвет изтъкна своето убеждение, че за тази цел е необходим новаторски подход към трансграничния обмен на информация в областта на правоприлагането.

(4) В тази връзка Европейският съвет заяви, че обменът на подобна информация следва да отговаря на условията, приложими към принципа на наличност. Това означава, че когато за изпълнение на служебните си задължения служител на правоприлагащ орган в една държава-членка на Съюза се нуждае от информация, той може да я получи от друга държава-членка и че правоприлагащите органи в държавата-членка, която притежава дадената информация, я предоставят за заявеното ѝ предназначение, вземайки предвид нуждите на висящите разследвания в тази държава-членка.

(5) Европейският съвет определи 1 януари 2008 г. за краен срок за постигане на тази цел на Програмата от Хага.

(6) С Рамково решение 2006/960/ПВР на Съвета от 18 декември 2006 г. за опростяване на обмена на информация и сведения между правоприлагащите органи на държавите-членки на Европейския съюз [2] вече бяха установени правилата, според които правоприлагащите органи на държавите-членки могат бързо и ефективно да обменят налична информация и сведения с цел провеждане на наказателни разследвания или наказателни разузнавателни операции.

(7) В Програмата от Хага за укрепване на свободата, сигурността и правосъдието същевременно се изтъква, че следва да се използва целият потенциал на новите технологии, както и че следва да има реципрочен достъп до националните бази данни, с уговорката, че нови централизирани европейски бази данни следва да се създават единствено въз основа на проучвания, доказали полезността си.

[1] Становище от 10 юни 2007 г. (все още непубликувано в Официален вестник).

[2] ОВ L 386, 29.12.2006 г., стр. 89.

(8) За ефективното международно сътрудничество е от изключително значение възможността за бърз и ефикасен обмен на точна информация. Целта е да се въведат процедури за насърчаване на бърз, ефикасен и нескъп начин за обмен на данни. За целите на съвместното използване на данни тези процедури следва да подлежат на отчетност и да включват подходящи гаранции по отношение на точността и сигурността на данните по време на предаването и съхранението им, като се предвиждат и процедури за записване на обменените данни и ограничения върху използването на обменената информация.

(9) Тези изисквания са изпълнени от Договора от Прюм. За да се изпълнят съществените изисквания на Програмата от Хага за всички държави-членки в поставените от нея срокове, разпоредбите на основните части от Договора от Прюм следва да станат приложими за всички държави-членки.

(10) Следователно настоящото решение съдържа разпоредби, които се основават на основните разпоредби на Договора от Прюм и са предназначени да подобрят обмена на информация, чрез който държавите-членки си предоставят взаимно права на достъп до своите автоматизирани файлове с ДНК анализи, автоматизирани системи за дактилоскопична идентификация и данни за регистрацията на превозните средства. Когато става въпрос за данни от националните файлове с ДНК анализи и автоматизирани системи за дактилоскопична идентификация, система на принципа „има/няма попадение“ следва да позволява на търсещата държава-членка, като втора стъпка, да изиска конкретни свързани лични данни от държавата-членка, администрираща файла, и когато е необходимо, да изиска допълнителна информация чрез процедури за взаимна помощ, включително приетите по силата на Рамково решение 2006/960/ПВР.

(11) Това ще ускори значително съществуващите процедури, защото ще даде възможност на държавите-членки да установят дали някоя от останалите държави-членки разполага с нужната ѝ информация и ако е така, коя от тях.

(12) Трансграничното сравняване на данни следва да разкрие ново измерение в борбата с престъпността. Информацията, получена чрез сравняване на данните, следва да предложи на държавите-членки нови подходи за разследване и по този начин да се превърне във важен фактор, подпомагащ дейността на техните правоприлагащи и съдебни органи.

(13) Правилата се основават на свързването в мрежа на националните бази данни на държавите-членки.

(14) При съблюдаване на определени условия държавите-членки следва да могат да предоставят лични и нелични данни с оглед подобряване обмена на информация във връзка с предотвратяването на престъпления и опазването на обществения ред и сигурността във връзка с големи събития с трансгранично измерение.

(15) При прилагането на член 12 държавите-членки могат да решат да дадат приоритет на борбата срещу тежките престъпления, имайки предвид ограничения наличен технически капацитет за предаване на информация.

(16) В допълнение към подобряването на обмена на информация е необходимо да се регламентират и другите форми на по-тясно сътрудничество между полицейските органи, по-специално посредством съвместни операции за сигурност (например съвместни патрули).

(17) По-тясното полицейско и съдебно сътрудничество по наказателноправни въпроси трябва да бъде съчетано със зачитане на основните права, по-специално правото на неприкосновеност на личния живот и защита на личните данни, което следва да се гарантира чрез специални договорености за защита на данните, които следва да са съобразени със специфичното естество на различните форми на обмен на данни. Такива разпоредби за защита на данните следва да вземат предвид спецификата на трансграничния онлайн-достъп до бази данни. Тъй като при режима на онлайн-достъп държавата-членка, администрираща файла, няма възможност да прави предварителни проверки, следва да е налице система, която да осигури последващ (*post hoc*) мониторинг.

(18) Системата на принципа „има/няма попадение“ предвижда структура за сравняване на анонимни профили, където допълнителните лични данни се обменят само след попадение, като предоставянето и получаването на тези данни се урежда от националното законодателство, включително от правилата за правна помощ. Тази уредба гарантира адекватна защита на данните, като се има предвид, че предоставянето на лични данни на друга държава-членка изисква подходящо ниво на защита на данните от страна на получаващите държави-членки.

(19) Имайки предвид обширния обмен на информация и данни в резултат на по-тясното полицейско и съдебно сътрудничество, настоящото решение има за цел да гарантира подходящо равнище на защита на данните. То съблюдава степента на защита, предвидена за обработване на лични данни от Конвенцията на Съвета на Европа за защита на физическите лица при автоматизираната обработка на лични данни от 28 януари 1981 г., допълнителния протокол към нея от 8 ноември 2001 г., както и принципите на Препоръка № R (87) 15 на Съвета на Европа относно използването на лични данни в полицейския сектор.

(20) Предвидените в настоящото решение разпоредби за защита на данните включват освен това принципите за защита на данните, които бяха необходими поради липсата на рамково решение относно защитата на данните в третия стълб. Настоящото рамково решение следва да се прилага спрямо цялото пространство на полицейското и съдебното сътрудничество по наказателноправни въпроси, при условие че осигурява степен на защита на данните, която не е по-малка от защитата, предвидена от Конвенцията на Съвета на Европа за защита на физическите лица при автоматизираната обработка на лични данни от 28 януари 1981 г. и допълнителния протокол към нея от 8 ноември 2001 г., като взема предвид Препоръка № R (87) 15 от 17 септември 1987 г. на Комитета на министрите към държавите-членки относно използването на данни в полицейския сектор, както и случаите, в които няма автоматизирана обработка на данни.

(21) Тъй като целите на настоящото решение, по-специално подобряването на информационния обмен в Европейския съюз, не могат да бъдат постигнати в достатъчна степен от отделните държави-членки поради трансграничното естество на борбата с престъпността и на въпросите на сигурността, поради което държавите-членки са длъжни да разчитат една на друга в тези области, и следователно тези цели могат да бъдат постигнати по-добре на равнището на Европейския съюз, Съветът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за създаване на Европейската общност, на който се позовава член 2 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в член 5 от Договора за ЕО, настоящото решение не надхвърля необходимото за постигането на тези цели.

(22) Настоящото решение зачита основните права и спазва принципите, установени по-специално в Хартата на Европейския съюз за основните права,

РЕШИ:

ГЛАВА 1

ОБЩИ ПОЛОЖЕНИЯ

Член 1

Цел и обхват

Чрез настоящото решение държавите-членки възнамеряват да засилят трансграничното сътрудничество по въпросите, уредени в дял VI от Договора, по-специално обмена на информация между органите, отговарящи за предотвратяването и разследването на престъпления. За тази цел настоящото решение съдържа правила в следните области:

а) разпоредби относно условията и процедурата за автоматично предаване на ДНК профили, дактилоскопични данни и определени данни от националната регистрация на превозните средства (глава 2);

б) разпоредби относно условията за предоставяне на данни, свързани с големи събития с трансгранично измерение (глава 3);

в) разпоредби относно условията за предоставяне на информация с цел предотвратяване на терористични престъпления (глава 4);

г) разпоредби относно условията и процедурата за засилване на трансграничното полицейско сътрудничество чрез различни мерки (глава 5).

ГЛАВА 2

ОНЛАЙН-ДОСТЪП И ПОСЛЕДВАЩИ ИСКАНИЯ

РАЗДЕЛ 1

ДНК профили

Член 2

Създаване на национални файлове с ДНК анализи

1. Държавите-членки създават и съхраняват национални файлове с ДНК анализи за разследване на престъпления. Обработката на данните, съхранявани в тези файлове съгласно настоящото решение, се извършва в съответствие с настоящото решение, при съобразяване с националното законодателство, приложимо към обработката.

2. С цел изпълнение на настоящото решение държавите-членки осигуряват наличието на справочни данни от техните национални файлове с ДНК анализи, както е посочено в параграф 1, първо изречение. Справочните данни включват само ДНК профили, създадени от некодиращата част на ДНК, и референтен номер. Справочните данни не съдържат никакви данни, чрез които субектът им може да бъде пряко идентифициран. Справочните данни, които не принадлежат на никое физическо лице („неидентифицирани ДНК профили“), следва да бъдат разпознаваеми като такива.

3. Всяка държава-членка информира генералния секретариат на Съвета за националните файлове с ДНК анализи, към които се прилагат членове 2—6, както и за условията за автоматизирано търсене, посочени в член 3, параграф 1, в съответствие с член 36.

Член 3

Автоматизирано търсене на ДНК профили

1. При разследването на престъпления държавите-членки разрешават на националните звена за контакт на други държави-членки, посочени в член 6, достъп до справочните данни в техните файлове с ДНК анализи, с правомощието да провеждат автоматизирано търсене чрез сравняване на ДНК профили. Търсене може да се осъществява само в отделни случаи и в съответствие с националното законодателство на молещата държава-членка.

2. Ако автоматизирано търсене покаже, че предоставен ДНК профил съвпада с ДНК профилите, въведени в претърсвания от получаващата държава-членка файл, тогава националното звено за контакт на търсещата държава-членка получава по автоматизиран път справочните данни, на които е намерено съвпадение. Когато не е намерено съвпадение, за това се изпраща автоматизирано съобщение.

Член 4

Автоматизирано сравняване на ДНК профили

1. При разследването на престъпления държавите-членки, по взаимно съгласие и чрез националните си звена за контакт, сравняват ДНК профилите от своите неидентифицирани ДНК профили с всички ДНК профили от другите справочни данни, съдържащи се в национални файлове с ДНК анализ. Профилите се предоставят и сравняват в автоматизирана форма. Неидентифицираните ДНК профили се предоставят за сравнение само в случаите, когато това е предвидено в националното законодателство на молещата държава-членка.

2. Когато държава-членка открие в резултат на сравнението, посочено в параграф 1, че някои предоставени ДНК профили съвпадат с профили от собствените ѝ файлове с ДНК анализи, тя незабавно предоставя на националното звено за контакт на другата държава-членка справочните данни, за които е намерено съвпадение.

Член 5

Предоставяне на допълнителни лични данни и друга информация

Когато процедурите, посочени в членове 3 и 4, покажат съвпадение между ДНК профили, предоставянето на допълнителни налични лични данни и друга информация, отнасяща се до справочните данни, се урежда от националното законодателство, включително от правилата за правна помощ на помолената държава-членка.

Член 6

Национално звено за контакт и мерки за изпълнение

1. За целите на предоставянето на данните, посочени в членове 3 и 4, всяка държава-членка определя национално звено за контакт. Правомощията на националните звена за контакт се уреждат от приложимото национално законодателство.

2. Подробностите за техническата уредба на процедурите, посочени в членове 3 и 4, се описват в мерките за изпълнение, посочени в член 33.

Член 7

Събиране на клетъчен материал и предоставяне на ДНК профили

Когато в текущо разследване или наказателно производство няма наличен ДНК профил за дадено лице на територията на помолената държава-членка, същата осигурява правна помощ, като събира и изследва клетъчен материал от това лице и предоставя получения ДНК профил, при условие че:

а) молещата държава-членка посочи причината, поради която изисква това;

б) молещата държава-членка представи заповед за разследване или изявление на компетентния орган, както е предвидено в законодателството на тази държава-членка, в което се посочва, че изискванията за събиране и изследване на клетъчен материал биха били изпълнени, ако съответното лице се намира на територията на молещата държава-членка; и

в) съгласно законодателството на помолената държава-членка са изпълнени изискванията за събиране и изследване на клетъчен материал и за предоставяне на получения ДНК профил.

РАЗДЕЛ 2

Дактилоскопични данни

Член 8

Дактилоскопични данни

С цел изпълнение на настоящото решение държавите-членки осигуряват наличието на справочни данни от файла за националните автоматизирани системи за дактилоскопична идентификация, създадени за предотвратяване и разследване на престъпления. Справочните данни включват само дактилоскопични данни и референтен номер. Справочните данни не съдържат никакви данни, чрез които субектът на данните може да бъде пряко идентифициран. Справочните данни, които не могат да бъдат отнесени към никое лице („неидентифицирани дактилоскопични данни“), следва да бъдат разпознаваеми като такива.

Член 9

Автоматизирано търсене на дактилоскопични данни

1. За предотвратяване и разследване на престъпления държавите-членки разрешават на националните звена за контакт на други държави-членки, посочени в член 11, достъп до справочните данни в създадените от тях за тази цел автоматизирани системи за дактилоскопична идентификация, с правомощието да провеждат автоматизирано търсене чрез сравняване на дактилоскопични данни. Търсенето може да се осъществява само в отделни случаи и в съответствие с националното законодателство на молещата държава-членка.

2. Потвърждаването на съвпадение на дактилоскопични данни със справочни данни, съхранявани от администриращата файла държава-членка, се осъществява от националното звено за контакт на молещата държава-членка посредством автоматизирано предоставяне на справочните данни, необходими за ясно съвпадение.

Член 10

Предоставяне на допълнителни лични данни и друга информация

Когато процедурата, посочена в член 9, покаже съвпадение между дактилоскопични данни, предоставянето на всякакви допълнителни налични лични данни и друга информация, отнасяща се до справочните данни, се урежда от националното законодателство, включително от правилата за правна помощ на помолената държава-членка.

Член 11

Национално звено за контакт и мерки за изпълнение

1. За целите на предоставянето на данни, предвидено в член 9, всяка държава-членка определя национално звено за контакт. Правомощията на националните звена за контакт се уреждат от приложимото национално законодателство.

2. Подробностите за техническата уредба на процедурата, посочена в член 9, се описват в мерките за изпълнение, посочени в член 33.

РАЗДЕЛ 3

Данни за регистрацията на превозните средства

Член 12

Автоматизирано търсене на данни за регистрацията на превозните средства

1. За предотвратяване и разследване на престъпления и в работата си по други нарушения, попадащи в юрисдикцията на съдилищата или на прокуратурата на търсещата държава-членка, както и за поддържане на обществената сигурност, държавите-членки предоставят на националните звена за контакт на други държави-членки, както е посочено в параграф 2, достъп до следните национални данни за регистрация на превозните средства, с правомощието да провеждат автоматизирано търсене в отделни случаи:

а) данни, свързани с притежатели или държатели; и

б) данни, свързани с превозни средства.

Търсенето може да се провежда само с пълен номер на шасито или пълен регистрационен номер. Търсенето може да се осъществява само в съответствие с националното законодателство на търсещата държава-членка.

2. За целите на предоставянето на данни, предвидено в параграф 1, всяка държава-членка определя национално звено за контакт по постъпващи искания. Правомощията на националните звена за контакт се уреждат от приложимото национално законодателство. Подробностите за техническата уредба на процедурата се описват в мерките за изпълнение, посочени в член 33.

ГЛАВА 3

ГОЛЕМИ СЪБИТИЯ

Член 13

Предоставяне на нелични данни

За предотвратяване на престъпления и за поддържане на обществения ред и сигурността по време на големи събития с трансгранично измерение, и по-специално спортни събития или заседания на Европейския съвет, държавите-членки, в съответствие с националното законодателство на предоставящата държава-членка, си предоставят взаимно всякакви нелични данни, изисквани за тези цели, както при поискване, така и по своя инициатива.

Член 14

Предоставяне на лични данни

1. За предотвратяване на престъпления и за поддържане на обществения ред и сигурността по време на големи събития с трансгранично измерение, по-специално спортни състезания или заседания на Европейския съвет, държавите-членки, както при поискване, така и по своя инициатива, си предоставят взаимно лични данни, ако постановените окончателни присъди или други обстоятелства дават основание да се счита, че субектите на данните ще извършат престъпление по време на събитието или представляват заплаха за обществения ред и сигурността, доколкото предоставянето на подобни данни е разрешено от националното законодателство на предоставящата държава-членка.

2. Личните данни могат да бъдат обработвани само за целите, посочени в параграф 1, и за конкретните събития, за които са предоставени. Предоставените данни трябва да се заличат незабавно след постигане на целите, посочени в параграф 1, или ако те са вече непостижими. Предоставените данни трябва във всички случаи да бъдат заличени след не повече от една година.

Член 15

Национално звено за контакт

За целите на предоставянето на данни, посочено в членове 13 и 14, всяка държава-членка определя национално звено за контакт. Правомощията на националните звена за контакт се уреждат от приложимото национално законодателство.

ГЛАВА 4

МЕРКИ ЗА ПРЕДОТВРАТЯВАНЕ НА ТЕРОРИСТИЧНИ ПРЕСТЪПЛЕНИЯ

Член 16

Предоставяне на информация с цел предотвратяване на терористични престъпления

1. За предотвратяването на терористични престъпления държавите-членки могат, в съответствие с националното им законодателство, в отделни случаи, дори да няма отправено искане към тях, да предоставят на посочените в параграф 3 национални звена за контакт на други държави-членки личните данни и информация, указани в параграф 2, доколкото това е необходимо, тъй като конкретни обстоятелства дават основание да се счита, че субектите на данните ще извършат престъпление, както е посочено в членове 1—3 от Рамково решение 2002/475/ПВР на Съвета от 13 юни 2002 г. относно борбата с тероризма ([1]).

([1]) ОВ L 164, 22.6.2002 г., стр. 3.

2. Предоставяните данни включват фамилия, първи имена, дата и място на раждане и описание на обстоятелствата, пораждащи убеждението, посочено в параграф 1.

3. Всяка държава-членка определя национално звено за контакт с цел обмен на информация с националните звена за контакт на другите държави-членки. Правомощията на националните звена за контакт се уреждат от приложимото национално законодателство.

4. Предоставящата държава-членка може, в съответствие с националното законодателство, да наложи условия за използването на подобни данни и информация от получаващата държава-членка. Тези условия обвързват получаващата държава-членка.

ГЛАВА 5

ДРУГИ ФОРМИ НА СЪТРУДНИЧЕСТВО

Член 17

Съвместни операции

1. За да засилят полицейското сътрудничество, определените от държавите-членки компетентни органи могат, при поддържане на обществения ред и сигурността, както и при предотвратяване на престъпления, да въвеждат съвместни патрули и други съвместни операции, в които определени служители или други длъжностни лица („служители“) от други държави-членки участват в операции на територията на държава-членка.

2. Всяка държава-членка може, като приемаща държава-членка, в съответствие със собственото си национално законодателство и със съгласието на изпращащата държава-членка, да предостави изпълнителни правомощия на служителите на изпращащата държава-членка, участващи в съвместни операции, или, доколкото позволява законодателството на приемащата държава-членка, да позволи на служителите от изпращащите държави-членки да упражняват техните изпълнителни правомощия в съответствие със законодателството на изпращащата държава-членка. Подобни изпълнителни правомощия могат да се упражняват само под ръководството на служителите от приемащата държава-членка и по правило — само в тяхно присъствие. Служителите на изпращащите държави-членки се подчиняват на националното законодателство на приемащата държава-членка. Приемащата държава-членка поема отговорност за техните действия.

3. Служителите на изпращащи държави-членки, които участват в съвместни операции, се подчиняват на инструкциите, дадени от компетентния орган на приемащата държава-членка.

4. Държавите-членки представят декларациите, посочени в член 36, в които посочват практическите аспекти на сътрудничеството.

Член 18

Съдействие във връзка с масови събирания, бедствия и сериозни произшествия

Компетентните органи на държавите-членки си оказват взаимно съдействие в съответствие с националното законодателство във връзка с масови събирания и подобни големи събития, както и във връзка с бедствия и сериозни произшествия, като се стремят да предотвратяват престъпления и да опазват обществения ред и сигурността, като:

а) взаимно се уведомяват възможно най-бързо за подобни ситуации с трансгранично въздействие и като обменят имаща отношение към случая информация;

б) предприемат и координират необходимите полицейски мерки в рамките на територията си при ситуации с трансгранично въздействие;

в) доколкото е възможно, изпращат служители, специалисти и консултанти, както и предоставят оборудване по искане на държавата-членка, на чиято територия е възникнала ситуацията.

Член 19

Употреба на оръжие, боеприпаси и оборудване

1. Служители от изпращаща държава-членка, които участват в съвместна операция на територията на друга държава-членка по силата на член 17 или 18, могат да носят в нея собствените си национални униформи. Те могат да носят такива оръжия, боеприпаси и оборудване, каквито им позволява националното законодателство на изпращащата държава-членка. Приемащата държава-членка може да забрани на служители от изпращащата държава-членка да носят определени оръжия, боеприпаси или оборудване.

2. Държавите-членки представят декларациите, посочени в член 36, в които се изброяват оръжията, боеприпасите и оборудването, които могат да се използват само при законна самоотбрана или за отбрана на други лица. Служителят на приемащата държава-членка, който отговаря за практическото извършване на операцията, може в отделни случаи и в съответствие с националното законодателство да издава разрешение за употреба на оръжие, боеприпаси и оборудване и за други цели, освен посочените в първото изречение. Употребата на оръжие, боеприпаси и оборудване се урежда от законодателството на приемащата държава-членка. Компетентните органи се информират взаимно за оръжието, боеприпасите и оборудването, които са разрешени, както и за условията за употребата им.

3. Ако служители от една държава-членка използват превозни средства в действия по настоящото решение на територията на друга държава-членка, те спазват същите правила за движение по пътищата, каквито и служителите на приемащата държава-членка, включително и по отношение на предимството по пътищата и всякакви други специални привилегии.

4. Държавите-членки представят декларациите, посочени в член 36, в които посочват практическите аспекти на употребата на оръжие, боеприпаси и оборудване.

Член 20

Защита и съдействие

От държавите-членки се изисква да предоставят на пресичащите границата служители от други държави-членки същата защита и съдействие в хода на изпълнение на техните задължения, каквато оказват и на собствените си служители.

Член 21

Общи правила за гражданска отговорност

1. Когато длъжностни лица на една държава-членка извършват операции съгласно член 17 в друга държава-членка, тяхната държава-членка носи отговорност за всички причинени от тях по време на техните операции вреди в съответствие със законодателството на държавата-членка, на чиято територия те извършват операциите.

2. Държавата-членка, на чиято територия е нанесена вредата, посочена в параграф 1, поправя тази вреда съгласно условията, приложими за вреди, причинени от собствените ѝ длъжностни лица.

3. В случая, предвиден в параграф 1, държавата-членка, чиито длъжностни лица са нанесли вреда на някое лице на територията на друга държава-членка, възстановяват на последната в пълен размер всички суми, които тя е заплатила на пострадалите или на упълномощените от тяхно име.

4. Когато длъжностни лица на една държава-членка извършват операции съгласно член 18 в друга държава-членка, последната носи отговорност в съответствие с националното си законодателство за всички вреди, нанесени от тях по време на техните операции.

5. Когато вредата, посочена в параграф 4, е резултат от груба небрежност или умишлено неправомерно поведение, приемащата държава-членка може да поиска от изпращащата държава-членка да ѝ бъдат възстановени всички суми, изплатени на пострадалите или на упълномощените от тяхно име.

6. Без да се засяга упражняването на правата ѝ по отношение на трети страни и с изключение на параграф 3, всяка държава-членка се въздържа в случая, предвиден в параграф 1, да иска обезщетение за вредите, които е претърпяла от друга държава-членка.

Член 22

Наказателна отговорност

Служителите, извършващи операции на територията на друга държава-членка съгласно настоящото решение, се третират по същия начин като служителите на приемащата държава-членка по отношение на всички престъпления, които може да са извършени от или срещу тях, освен ако не е предвидено друго в друго споразумение с обвързващ характер за съответните държави-членки.

Член 23

Трудови правоотношения

Спрямо служителите, извършващи операции на територията на друга държава-членка съгласно настоящото решение, се прилагат разпоредбите на трудовото право, приложими в тяхната собствена държава-членка, по-специално онези, които касаят дисциплинарните правила.

ГЛАВА 6

ОБЩИ РАЗПОРЕДБИ ЗА ЗАЩИТА НА ДАННИТЕ

Член 24

Определения и обхват

1. За целите на настоящото решение:

а) „обработка на лични данни“ означава всякаква операция или набор от операции, извършвани със или без автоматизирани средства по отношение на личните данни, като събиране, записване, организиране, съхранение, адаптиране или промяна, сортиране, извличане, консултиране, употреба, разкриване чрез предоставяне, разпространяване или друга форма на предоставяне, равняване, комбиниране, блокиране, изтриване или унищожаване на данни. Обработката по смисъла на настоящото решение включва и уведомяване за това, дали има или няма попадение;

б) „автоматизирана процедура за търсене“ означава пряк достъп до автоматизираните файлове на друг орган, при който отговорът на процедурата по търсенето е напълно автоматизиран;

в) „обозначаване“ означава маркирането на съхранените лични данни, без да се цели ограничаване на тяхната обработка в бъдеще;

г) „блокиране“ означава маркирането на съхранените лични данни с цел ограничаване на тяхната обработка в бъдеще.

2. Следните разпоредби се прилагат към данни, които се предоставят или са били предоставени в съответствие с настоящото решение, освен ако в предходните глави не е предвидено друго.

Член 25

Степен на защита на данните

1. По отношение на обработката на лични данни, които се предоставят или са били предоставени в съответствие с настоящото решение, всяка държава-членка осигурява степен на защита на личните данни в националното си законодателство, която е най-малкото равностойна на тази, произтичаща от Конвенцията на Съвета на Европа за защита на физическите лица при автоматизираната обработка на лични данни от 28 януари 1981 г. и допълнителния протокол към нея от 8 ноември 2001 г., като взема предвид Препоръка № R (87) 15 от 17 септември 1987 г. на Комитета на министрите на Съвета на Европа към държавите-членки, регламентираща използването на лични данни в полицейския сектор, както и случаите, в които няма автоматизирана обработка на данни.

2. Предоставянето на лични данни, предвидено в настоящото решение, не може да се осъществи преди разпоредбите в настоящата глава да са въведени в националното законодателство на територията на държавите-членки, участващи в подобно предоставяне. Съветът решава единодушно дали това условие е спазено.

3. Параграф 2 не се прилага към тези държави-членки, в които предоставянето на лични данни, предвидено в настоящото решение, е започнало съгласно Договора от 27 май 2005 г. между Кралство Белгия, Федерална република Германия, Кралство Испания, Френската република, Великото херцогство Люксембург, Кралство Нидерландия и Република Австрия относно засилването на трансграничното сътрудничество, по-специално в борбата срещу тероризма, трансграничната престъпност и незаконната миграция („Договора от Прюм“).

Член 26

Цел

1. Обработката на лични данни от получаващата държава-членка се разрешава единствено за целите, за които са предоставени данните, в съответствие с настоящото решение. Обработката за други цели се разрешава единствено с предварителното разрешение на държавата-членка, администрираща файла, и се подчинява само на националното законодателство на получаващата държава-членка. Такова разрешение може да бъде дадено, при условие че в националното законодателство на държавата-членка, администрираща файла, е разрешена обработката за такива други цели.

2. Обработката на данни, предоставени в съответствие с членове 3, 4 и 9, от страна на търсещата или сравняващата държава-членка, се разрешава единствено за да се:

а) установи дали има съвпадение между сравняваните ДНК профили или дактилоскопични данни;

б) изготви и подаде полицейско или съдебно искане за правна помощ в съответствие с националното законодателство, когато тези данни съвпадат;

в) направи запис по смисъла на член 30.

Държавата-членка, която администрира файла, може да обработи предоставените ѝ в съответствие с членове 3, 4 и 9 данни само когато това е необходимо с цел сравнение, като предоставя автоматизирани отговори на търсения или записи, извършени в съответствие с член 30. Предоставените данни се заличават непосредствено след сравняването на данните след получаването на автоматизирани отговори на търсене, освен когато се налага понататъшна обработка за целите, посочени в първа алинея, букви б) и в).

3. Данните, предоставени в съответствие с член 12, могат да се използват от държавата-членка, администрираща файла, само когато това е необходимо с цел предоставяне на автоматизирани отговори на процедури по търсене или запис, както е посочено в член 30. Предоставените данни се заличават непосредствено след получаването на автоматизираните отговори на търсенето, освен ако не е необходима допълнителна обработка на запис съгласно член 30. Търсещата държава-членка може да използва получените данни в отговор само за процедурата, за която е извършила търсенето.

Член 27

Компетентни органи

Предоставените лични данни могат да се обработват само от властите, органите и съдилищата, които са натоварени със задачи по изпълнение на целите, посочени в член 26. По-специално, данните могат да бъдат предоставени на други лица само с предварителното разрешение на предоставящата държава-членка и в съответствие със законодателството на получаващата държава-членка.

Член 28

Точност, актуалност и срок за съхранение на данните

1. Държавите-членки осигуряват точността и актуалността на личните данни. Ако стане известно *ex officio* или от уведомление от субекта на данните, че са предоставени погрешни данни или данни, които не е трябвало да бъдат предоставени, това се съобщава незабавно на получаващата(ите) държава(и)-членка(и). Въпросната(ите) държава(и)-членка(и) е(са) длъжна(и) да коригира(т) или заличи(ат) данните. Освен това предоставените лични данни се коригират, ако се установи, че са погрешни. Ако получаващият информацията орган има основания да счита, че предоставените данни са погрешни или че трябва да се заличат, предоставящият ги орган следва да бъде уведомен за това.

2. Данни, чиято точност се оспорва от субекта на данните и чиято точност или неточност не може да бъде установена, се маркират с флагче по искане на субекта на данните в съответствие с националното законодателство на държавите-членки. Ако е налице флагче, то може да бъде отстранено в съответствие с националното законодателство на държавите-членки и само с разрешението на субекта на данните въз основа или на решение на компетентен съд, или на независим орган за защита на данните.

3. Предоставени лични данни, които не е трябвало да бъдат предоставени или получени, се заличават. Законно предоставени и получени данни се заличават:

а) ако не са или вече не са необходими за целта, за която са предоставени; ако са били предоставени лични данни, които не са били поискани, получаващият орган незабавно проверява дали те са необходими за целите, за които са били предоставени;

б) след изтичане на максималния срок за съхранение на данни, предвиден в националното законодателство на предоставящата ги държава-членка, ако предоставящият орган е информирал получаващия орган за тези максимални срокове към момента на предоставяне на данните.

Когато има основание да се счита, че заличаването ще увреди интересите на субекта на данните, вместо да бъдат заличени, данните се блокират в съответствие с националното законодателство. Блокираните данни могат да се предоставят или използват единствено за целта, която е предотвратила тяхното заличаване.

Член 29

Технически и организационни мерки за осигуряване на защитата и сигурността на данните

1. Предоставящите и получаващите органи предприемат стъпки, за да осигурят ефективната защита на личните данни от случайно или неразрешено унищожаване, случайна загуба, неразрешен достъп, неразрешено или случайно изменение и неразрешено разкриване.

2. Особеностите на техническата спецификация на процедурата за автоматизирано търсене се уреждат в мерките за изпълнение, посочени в член 33, които гарантират, че:

а) се предприемат модерни технически мерки, за да се осигури защитата и сигурността на данните, по-специално тяхната поверителност и неприкосновеност;

б) се използват признати от компетентните органи процедури за криптиране и разрешаване, когато се използват общодостъпни мрежи; и

в) допустимостта на търсене в съответствие с член 30, параграфи 2, 4 и 5, може да бъде проверена.

Член 30

Протоколиране и записване; специални правила, уреждащи автоматизираното и неавтоматизираното предоставяне

1. Всяка държава-членка гарантира, че всяко неавтоматизирано предоставяне и всяко неавтоматизирано получаване на лични данни от администриращия файла орган и от търсещия орган се протоколира, за да се удостовери допустимостта на предоставянето. Протоколът включва следната информация:

а) основанието за предоставяне;

б) предоставените данни;

в) датата на предоставяне; и

г) името или референтния номер на търсещия орган и на органа, администриращ файла.

2. Следното се отнася до автоматизираното търсене на данни въз основа на членове 3, 9 и 12 и до автоматизираното сравняване съгласно член 4:

а) само специално оправомощени служители на националните звена за контакт могат да извършват автоматизирано търсене или сравняване. Списъкът на служителите, оправомощени да извършват автоматизирано търсене или сравняване, се предоставя при поискване на надзорните органи, посочени в параграф 5, и на другите държави-членки;

б) всяка държава-членка гарантира, че всяко предоставяне и получаване на лични данни от органа, администриращ файла, и от търсещия орган се записва, като включително се отбелязва дали има или няма попадение. Записът включва следната информация:

i) предоставените данни;

ii) датата и точното време на предоставяне; и

iii) наименованието или референтния номер на търсещия орган и на органа, администриращ файла.

Освен това търсещият орган записва основанието за търсене или предоставяне, идентификатора на служителя, провел търсенето, и този на служителя, поръчал търсенето или предоставянето.

3. При поискване органът, който прави записа, незабавно съобщава записаните данни на компетентните органи по защита на данните на съответната държава-членка, най-късно до четири седмици след получаване на искането. Записаните данни могат да се използват само за следните цели:

а) наблюдение на защитата на данните;

б) гарантиране на сигурността на данните.

4. Записаните данни се защитават с подходящи мерки срещу неуместна употреба и други форми на неправилна употреба и се съхраняват в продължение на две години. След изтичането на срока на съхранение записаните данни се заличават незабавно.

5. Отговорността за проверка на законността на предоставянето или получаването на лични данни се носи от независимите органи за защита на данните или, когато е уместно, от съдебните органи на съответните държави-членки. Всеки може да поиска от тези органи да проверят законността на обработката на данни по отношение на неговата личност в съответствие с националното законодателство. Независимо от подобни искания тези органи и органите, отговарящи за записването, провеждат случайни проверки на законността на предоставянето въз основа на използваните файлове.

Резултатите от подобни проверки се съхраняват с цел инспекция от независимите органи за защита на данните в продължение на 18 месеца. След изтичането на този срок те се заличават незабавно. От всеки независим орган за защита на данните може да бъде поискано от независим орган за защита на данните на друга държава-членка да упражни правомощията си в съответствие с националното законодателство. Независимите органи за защита на данните на държавите-членки извършват инспекционните задачи, необходими за взаимно сътрудничество, по-специално чрез обмяна на подходяща информация.

Член 31

Права на субектите на данни на информация и обезщетения

1. По искане на субекта на данните съгласно националното законодателство му се предоставя информация в съответствие с националното законодателство на този субект срещу представяне на доказателство за неговата самоличност, без неоснователни разходи, в разбираема форма и без неприемливо закъснение относно данните, обработени по отношение на неговата личност, произхода на данните, получателя или групите получатели, предвидената цел на обработката и, когато това се изисква от националното законодателство, правното основание за обработката. Освен това субектът на данните има правото на поправка на неточни данни и на заличаване на незаконно обработени данни. Държавите-членки също гарантират, че в случай на нарушение на правата му във връзка със защита на данните, субектът на данните има възможност да подаде жалба до независим съд или трибунал по смисъла на член 6, параграф 1 от Европейската конвенция за правата на човека или до независим надзорен орган по смисъла на член 28 от Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ([1]) и че той е получил възможността да подаде иск за щети или да потърси друга форма на законна компенсация. Подробните правила относно процедурата за упражняване на тези права и основанията за ограничаване правото на достъп се уреждат от съответните национални правни разпоредби на държавата-членка, в която субектът на данните упражнява своите права.

2. Когато орган на една държава-членка е предоставил лични данни по силата на настоящото решение, получаващият орган на другата държава-членка не може да използва неточността на предоставените данни като основание да избегне отговорността спрямо ощетената страна съгласно националното законодателство. Ако срещу получаващия орган бъдат присъдени щети поради използвани от него неточни предоставени данни, органът, който е предоставил данните, възстановява на получаващия орган пълния размер на изплатеното от него обезщетение.

Член 32

Информация, поискана от държавите-членки

Получаващата държава-членка по искане на предоставящата държава-членка я информира за обработката на предоставените данни и за получения резултат.

ГЛАВА 7

РАЗПОРЕДБИ ЗА ИЗПЪЛНЕНИЕ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 33

Мерки за изпълнение

Съветът приема с квалифицирано мнозинство и след консултация с Европейския парламент мерките, необходими за изпълнение на настоящото решение на равнището на Европейския съюз.

Член 34

Разходи

Всяка държава-членка поема оперативните разходи, направени от нейните органи във връзка с прилагането на настоящото решение. В специални случаи заинтересованите държави-членки могат да постигнат различни договорености.

Член 35

Връзка с други правни инструменти

1. Спрямо заинтересованите държави-членки се прилагат имащите отношение към тях разпоредби на настоящото решение вместо съответстващите им разпоредби, съдържащи се в Договора от Прюм. Всички други разпоредби от Договора от Прюм остават приложими между договарящите страни по него.

2. Без да се засягат ангажиментите им по други актове, приети съгласно дял VI от Договора:

а) Държавите-членки могат да продължат да прилагат двустранните или многостранни споразумения или договорености за трансгранично сътрудничество, които са в сила към датата на приемане на настоящото решение, доколкото подобни споразумения или договорености не са несъвместими с неговите цели.

б) Държавите-членки могат да сключват или привеждат в сила двустранни или многостранни споразумения или договорености за трансгранично сътрудничество след влизането в сила на настоящото решение, доколкото подобни споразумения или договорености предвиждат удължаване или разгръщане на целите на настоящото решение.

3. Споразуменията и договореностите, посочени в параграфи 1 и 2, не могат да засягат взаимоотношенията с държави-членки, които не са страни по тях.

4. В срок от четири седмици от пораждането на действие на настоящото решение държавите-членки информират Съвета и Комисията за съществуващите споразумения или договорености по смисъла на параграф 2, буква а), които те желаят да продължат да прилагат.

5. Държавите-членки също информират Съвета и Комисията за всякакви нови споразумения или договорености по смисъла на параграф 2, буква б), в рамките на три месеца от подписването им, или в случая на правни инструменти, които са подписани преди приемането на настоящото решение, в рамките на три месеца от тяхното влизане в сила.

6. Нищо в настоящото решение не засяга двустранните или многостранни споразумения или договорености между държавите-членки и трети държави.

7. Настоящото решение не засяга съществуващите споразумения за правна помощ или за взаимно признаване на съдебни решения.

([1]) ОВ L 281, 23.11.1995 г., стр. 31. Директива, изменена с Регламент (ЕО) № 1882/2003 (ОВ L 284, 31.10.2003 г., стр. 1).

Член 36

Изпълнение и декларации

1. Държавите-членки предприемат необходимите мерки, за да се съобразят с разпоредбите на настоящото решение в рамките на една година от пораждането на действие на настоящото решение, с изключение на разпоредбите на глава 2, по отношение на които необходимите мерки ще бъдат предприети в рамките на три години от пораждането на действие на настоящото решение и на решението на Съвета относно изпълнението на настоящото решение.

2. Държавите-членки информират генералния секретариат на Съвета и Комисията, че са изпълнили наложените им по силата на настоящото решение задължения и са представили предвидените в него декларации. При това всяка държава-членка може да посочи, че ще започне да прилага незабавно настоящото решение в отношенията си с онези държави-членки, които са подали същата нотификация.

3. Декларациите, представени в съответствие с параграф 2, могат да се изменят по всяко време посредством декларация, подадена до генералния секретариат на Съвета. Генералният секретариат на Съвета изпраща получените декларации на държавите-членки и на Комисията.

4. На основата на тази и на друга информация, предоставена от държавите-членки при поискване, до 28 юли 2012 г. Комисията предоставя на Съвета доклад относно изпълнението на настоящото решение, придружен от предложенията, които е сметнала за подходящи за по-нататъшно развитие.

Член 37

Прилагане

Настоящото решение поражда действие двадесет дни след публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Люксембург на 23 юни 2008 година.

За Съвета

Председател

I. JARC

РЕШЕНИЕ 2008/616/ПВР НА СЪВЕТА

от 23 юни 2008 година

за изпълнение на Решение 2008/615/ПВР относно засилването на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид член 33 от Решение 2008/615/ПВР на Съвета ([1]),

като взе предвид инициативата на Федерална република Германия,

като взе предвид становището на Европейския парламент ([2]),

като има предвид, че:

(1) На 23 юни 2008 г. Съветът прие Решение 2008/615/ПВР относно засилването на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност.

(2) С Решение 2008/615/ПВР основните елементи на Договора от 27 май 2005 г. между Кралство Белгия, Федерална република Германия, Кралство Испания, Френската република, Великото херцогство Люксембург, Кралство Нидерландия и Република Австрия относно засилването на трансграничното сътрудничество, по-специално в борбата срещу тероризма, трансграничната престъпност и нелегалната миграция (наричан по-долу „Договора от Прюм“), бяха транспонирани в правната рамка на Европейския съюз.

(3) Член 33 от Решение 2008/615/ПВР предвижда, че Съветът следва да приеме мерките, необходими за изпълнение на Решение 2008/615/ПВР на равнище Европейски съюз, в съответствие с процедурата, установена в член 34, параграф 2, буква в), второ изречение от Договора за Европейския съюз. Тези мерки следва да се основават на споразумението за изпълнение от 5 декември 2006 г. относно административното и техническото изпълнение и прилагане на Договора от Прюм.

(4) Настоящото решение установява тези общи нормативни разпоредби, които са необходими за административното и техническото изпълнение на формите на сътрудничество, установени в Решение 2008/615/ПВР. Приложението към настоящото решение съдържа изпълнителни разпоредби от технически характер. Освен това генералният секретариат на Съвета ще състави и поддържа актуален отделен наръчник, съдържащ главно фактическа информация, която следва да бъде предоставена от държавите-членки.

(5) Като се отчитат техническите способности, рутинното търсене на нови ДНК профили ще се осъществява по принцип с помощта на единични търсения, като подходящите решения в тази насока ще се търсят на техническо равнище,

РЕШИ:

ГЛАВА I

ОБЩИ ПОЛОЖЕНИЯ

Член 1

Цел

Целта на настоящото решение е да установи необходимите административни и технически разпоредби за изпълнение на Решение 2008/615/ПВР, по-специално по отношение на автоматизирания обмен на ДНК данни, дактилоскопични данни и данни за регистрацията на превозни средства, установени в глава 2 от посоченото решение, както и други форми на сътрудничество, установени в глава 5 от посоченото решение.

Член 2

Определения

За целите на настоящото решение:

а) „търсене“ и „сравняване“ съгласно посоченото в членове 3, 4 и 9 от Решение 2008/615/ПВР означават процедури, чрез които се установява дали има съвпадение съответно между ДНК данни или дактилоскопични данни, които са били съобщени от една държава-членка, и ДНК данни или дактилоскопични данни, съхранявани в базите данни на една, няколко или всички държави-членки;

б) „автоматизирано търсене“ съгласно посоченото в член 12 от Решение 2008/615/ПВР означава процедура за онлайн-достъп за справка в базите данни на една, няколко или всички държави-членки;

в) „ДНК профил“ означава буква или числов код, който представлява набор от идентификационни характеристики на некодиращата част на анализирана проба човешка ДНК, т.е. определена молекулярна структура в различните части на ДНК (локуси);

г) „некодираща част от ДНК“ означава хромозомни сектори, които нямат генетичен израз, т.е. за тях не е известно да осигуряват функционални свойства на даден организъм;

([1]) Вж. страница 1 от настоящия брой на Официален вестник.

([2]) Становище от 21 април 2008 г. (все още непубликувано в Официален вестник).

д) „референтни ДНК данни“ означава ДНК профил и референтен номер;

е) „референтен ДНК профил“ означава ДНК профил на идентифицирано лице;

ж) „неидентифициран ДНК профил“ означава ДНК профил, получен от следи, събрани по време на разследване на престъпления и принадлежащи на лице, което все още не е идентифицирано;

з) „забележка“ означава маркиране на ДНК профил от държава-членка в нейната национална база данни, посочващо, че вече е имало съвпадение на този ДНК профил при търсене или сравняване от друга държава-членка;

и) „дактилоскопични данни“ означава образи на пръстови отпечатъци, образи на следи от пръстови отпечатъци, отпечатъци на длани, следи на отпечатъци от длани, както и модели на такива образи (кодирани признаци (*minutiae*), когато те се съхраняват и обработват чрез автоматизирана база данни;

й) „данни за регистрацията на превозни средства“ означава съвкупността от данни, посочени в глава 3 от приложението към настоящото решение;

к) „отделен случай“, както е посочено в член 3, параграф 1, второ изречение, член 9, параграф 1, второ изречение и член 12, параграф 1 от Решение 2008/615/ПВР, означава отделно следствено дело или прокурорска преписка. В случай че такова дело или преписка съдържа повече от един ДНК профил или повече от един елемент от дактилоскопични данни или данни за регистрацията на превозно средство, те могат да бъдат изпратени заедно като едно искане.

ГЛАВА 2

ОБЩИ РАЗПОРЕДБИ ЗА ОБМЕН НА ДАННИ

Член 3

Технически спецификации

Държавите-членки спазват общите технически спецификации във връзка с всички искания и отговори, свързани с търсене и сравняване на ДНК профили, дактилоскопични данни и данни за регистрацията на превозни средства. Тези технически спецификации са посочени в приложението към настоящото решение.

Член 4

Комуникационна мрежа

Електронният обмен на ДНК данни, дактилоскопични данни и данни за регистрацията на превозни средства между държавите-членки се осъществява чрез използване на комуникационната мрежа за трансевропейски телематични услуги между администрациите (TESTA II) и нейните бъдещи версии.

Член 5

Достъпност на автоматизирания обмен на данни

Държавите-членки вземат всички необходими мерки, за да гарантират, че автоматизираното търсене или сравняване на ДНК данни, дактилоскопични данни и данни за регистрацията на превозни средства е възможно 24 часа в денонощието и седем дни в седмицата. В случай на техническа неизправност националните точки за контакт на държавите-членки незабавно се информират помежду си и се договарят за временни алтернативни механизми за информационен обмен в съответствие с приложимите законови разпоредби. Автоматизираният обмен на данни се възстановява възможно най-бързо.

Член 6

Референтни номера за ДНК данни и дактилоскопични данни

Референтните номера, посочени в членове 2 и 8 от Решение 2008/615/ПВР, представляват комбинация от следното:

а) код, позволяващ на държавите-членки, в случай на съвпадение, да извличат лични данни и друга информация от техните бази данни за да ги предоставят на една, няколко или всички държави-членки в съответствие с член 5 или 10 от Решение 2008/615/ПВР;

б) код за обозначаване на националния произход на ДНК профила или дактилоскопичните данни; и

в) по отношение на ДНК данните, код за обозначаване на типа на ДНК профила.

ГЛАВА 3

ДНК ДАННИ

Член 7

Принципи на обмен на ДНК данни

1. Държавите-членки използват съществуващите стандарти за обмен на ДНК данни, като европейския стандартен набор (ESS) или стандартния набор на Интерпол за справка по локуси (ISSOL).

2. Процедурата за предаване в случай на автоматизирано търсене и сравняване на ДНК профили се извършва в рамките на децентрализирана структура.

3. За да се гарантират поверителността и целостта на изпратените в други държави-членки данни, се вземат подходящи мерки, включително тяхното криптиране.

4. Държавите-членки вземат необходимите мерки, за да гарантират целостта на ДНК профилите, до които е даден достъп или които са изпратени на другите държави-членки за сравняване, а също и да гарантират, че тези мерки съответстват на международните стандарти, като ISO 17025.

5. Държавите-членки използват кодове за държава-членка в съответствие със стандарта ISO 3166-1 alpha-2.

Член 8

Правила за искания и отговори във връзка с ДНК данни

1. Искането за автоматизирано търсене или сравняване, съгласно член 3 или 4 от Решение 2008/615/ПВР, включва само следната информация:

а) кода на държавата-членка за отправилата искането държава-членка;

б) датата, часа и индикационния номер на искането;

в) ДНК профилите и техните референтни номера;

г) типа на предаваните ДНК профили (неидентифицирани ДНК профили или референтни ДНК профили); и

д) информацията, необходима за контролиране на системите от бази данни и за качествения контрол на процесите на автоматизирано търсене.

2. Отговорът (съобщение за съвпадение) на искането, посочено в параграф 1, съдържа само следната информация:

а) означение дали има едно или повече съвпадения (попадения) или няма съвпадения (няма попадение);

б) датата, часа и индикационния номер на искането;

в) датата, часа и индикационния номер на отговора;

г) кодовете на отправилата искането държава-членка и на държавата-членка, до която е отправено искането;

д) референтните номера на отправилата искането държава-членка и на държавата-членка, до която е отправено искането;

е) типа на предаваните ДНК профили (неидентифицирани ДНК профили или референтни ДНК профили);

ж) поисканите и съвпадащите ДНК профили; и

з) информацията, необходима за контролиране на системите от бази данни и за качествения контрол на процесите на автоматизирано търсене.

3. Автоматизирано уведомление за съвпадение се предоставя само ако при автоматизираното търсене или сравняване е установено съвпадение на определен минимален брой локуси. Този минимален брой е определен в глава 1 от приложението към настоящото решение.

4. Държавите-членки гарантират съответствието на отправените искания с декларациите, направени съгласно член 2, параграф 3 от Решение 2008/615/ПВР. Тези декларации се възпроизвеждат в наръчника, посочен в член 18, параграф 2 от настоящото решение.

Член 9

Процедура за предаване при автоматизирано търсене на неидентифицирани ДНК профили в съответствие с член 3 от Решение 2008/615/ПВР

1. Ако при търсене с неидентифициран ДНК профил в националната база данни не се установи съвпадение или се установи съвпадение с неидентифициран ДНК профил, неидентифицираният ДНК профил може впоследствие да бъде изпратен до базите данни на всички други държави-членки и ако при търсене с този неидентифициран ДНК профил се установят съвпадения с референтни ДНК профили и/или неидентифицирани ДНК профили в базите данни на други държави-членки, тези съвпадения се съобщават автоматично, а референтните ДНК данни се изпращат на отправилата искането държава-членка; в случай че в базите данни на други държави-членки не могат да се установят съвпадения, това се съобщава автоматично на отправилата искането държава-членка.

2. Ако при търсене с неидентифициран ДНК профил в базите данни на други държави-членки се установи съвпадение, всяка заинтересована държава-членка може да отбележи това със забележка в националната си база данни.

Член 10

Процедура за предаване при автоматично търсене на референтни ДНК профили в съответствие с член 3 от Решение 2008/615/ПВР

Ако при търсене с референтен ДНК профил в националната база данни не се установи съвпадение с референтен ДНК профил или се установи съвпадение с неидентифициран ДНК профил, този референтен ДНК профил може впоследствие да бъде изпратен до базите данни на всички други държави-членки и ако при търсене с този референтен ДНК профил се установят съвпадения с референтни ДНК профили и/или неидентифицирани ДНК профили в базите данни на други държави-членки, тези съвпадения се съобщават автоматично, а референтните ДНК данни се изпращат на отправилата искането държава-членка; ако в базите данни на други държави-членки не могат да се установят съвпадения, това се съобщава автоматично на отправилата искането държава-членка.

Член 11

Процедура за предаване при автоматизирано сравняване на неидентифицирани ДНК профили в съответствие с член 4 от Решение 2008/615/ПВР

1. Ако при сравняване с неидентифицирани ДНК профили в базите данни на други държави-членки се установят съвпадения с референтни ДНК профили и/или неидентифицирани ДНК профили, тези съвпадения се съобщават автоматично, а референтните ДНК данни се изпращат на отправилата искането държава-членка.

2. Ако при сравняване с неидентифицирани ДНК профили в базите данни на други държави-членки се установят съвпадения с неидентифицирани ДНК профили или с референтни ДНК профили, всяка заинтересована държава-членка може да отбележи това със забележка в националната си база данни.

ГЛАВА 4

ДАКТИЛОСКОПИЧНИ ДАННИ

Член 12

Принципи при обмена на дактилоскопични данни

1. Дигитализацията на дактилоскопични данни и тяхното предаване на другите държави-членки се осъществяват в съответствие с единния формат за данни, определен в глава 2 от приложението към настоящото решение.

2. Всяка държава-членка гарантира, че предаваните от нея дактилоскопични данни са с достатъчно добро качество за сравняване чрез автоматизираните системи за дактилоскопична идентификация (AFIS).

3. Процедурата за предаване при обмен на дактилоскопични данни се извършва в рамките на децентрализирана структура.

4. За да се гарантират поверителността и целостта на изпращаните към други държави-членки дактилоскопични данни, се вземат подходящи мерки, включително криптирането им.

5. Държавите-членки използват кодове за държава-членка в съответствие със стандарта ISO 3166-1 alpha-2.

Член 13

Капацитет за търсене на дактилоскопични данни

1. Всяка държава-членка гарантира, че нейните искания за търсене не превишават капацитета за търсене, посочен от държавата-членка, до която е отправено искането. Държавите-членки подават до генералния секретариат на Съвета декларации съгласно посоченото в член 18, параграф 2, в които заявяват максималния си капацитет на ден за търсене на дактилоскопични данни на идентифицирани лица и на дактилоскопични данни на все още неидентифицирани лица.

2. Максималният брой кандидатури, приемани за проверка при едно предаване, е установен в глава 2 от приложението към настоящото решение.

Член 14

Правила за искания и отговори във връзка с дактилоскопични данни

1. Държавата-членка, до която е отправено искането, незабавно проверява качеството на предадените дактилоскопични данни по напълно автоматизирана процедура. Ако данните не са подходящи за автоматизирано сравняване, държавата-членка, до която е отправено искането, информира незабавно отправилата искането държава-членка.

2. Държавата-членка, до която е отправено искането, извършва търсенията по реда на постъпване на исканията. Исканията се обработват в рамките на 24 часа чрез напълно автоматизирана процедура. Отправилата искането държава-членка може, ако националното ѝ право предвижда това, да помоли за ускорена обработка на нейното искане, а държавата-членка, до която е отправено искането, извършва незабавно търсенето. Ако поради непреодолима сила срокът не може да бъде спазен, сравняването се извършва незабавно след отстраняване на пречките.

ГЛАВА 5

ДАННИ ЗА РЕГИСТРАЦИЯТА НА ПРЕВОЗНИ СРЕДСТВА

Член 15

Принципи при автоматизирано търсене на данни за регистрацията на превозни средства

1. При автоматизирано търсене на данни за регистрацията на превозни средства, държавите-членки използват версия на софтуерното приложение към Европейската информационна система за превозни средства и свидетелства за управление (EUCARIS), специално разработено за целите на член 12 от Решение 2008/615/ПВР, както и измененитe версии на същия софтуер.

2. Автоматизираното търсене на данни за регистрацията на превозни средства се извършва в рамките на децентрализирана структура.

3. Обменената посредством системата EUCARIS информация се изпраща в криптирана форма.

4. Елементите на данните за регистрацията на превозни средства, които подлежат на обмен, са посочени в глава 3 от приложението към настоящото решение.

5. При изпълнението на член 12 от Решение 2008/615/ПВР държавите-членки могат да дадат приоритет на търсенията, свързани с борбата срещу тежките престъпления.

Член 16

Разходи

Всяка държава-членка поема разходите, произтичащи от администрирането, използването и поддръжката на софтуерното приложение на EUCARIS, посочено в член 15, параграф 1.

ГЛАВА 6

ПОЛИЦЕЙСКО СЪТРУДНИЧЕСТВО

Член 17

Съвместни патрули и други съвместни операции

1. В съответствие с глава 5 от Решение 2008/615/ПВР, и по-специално с декларациите, подадени съгласно член 17, параграф 4 и член 19, параграфи 2 и 4 от посоченото решение, всяка държава-членка посочва една или повече точки за контакт, за да

даде възможност на другите държави-членки да се обръщат към компетентни органи, и всяка държава-членка може да посочи своите процедури за установяване на съвместни патрули и други съвместни операции, процедурите си относно инициативите на други държави-членки във връзка с тези операции, както и други практически аспекти и реда и другите оперативни условия по отношение на тези операции.

2. Генералният секретариат на Съвета съставя и поддържа актуализиран списък на точките за контакт и информира компетентните органи за всяка промяна в този списък.

3. Компетентните органи на всяка държава-членка могат да предприемат инициатива за осъществяване на съвместна операция. Преди началото на конкретна операция компетентните органи, посочени в параграф 2, се договарят писмено или устно за подробности, като:

а) компетентните органи на държавите-членки за операцията;

б) конкретната цел на операцията;

в) държавата-членка домакин, в която трябва да се проведе операцията;

г) географската област от държавата-членка домакин, където трябва да се проведе операцията;

д) периодът, който обхваща операцията;

е) конкретната помощ, която да бъде предоставена от командироващата(ите) държава(и)-членка(и) на държавата-членка домакин, включително служители и друг персонал, материални и финансови ресурси;

ж) служителите, участващи в операцията;

з) служителят отговарящ за операцията;

и) правомощията, които служителите и други длъжностни лица от командироващата(ите) държава(и)-членка(и) могат да упражняват в държавата-членка домакин по време на операцията;

й) конкретното въоръжение, боеприпаси и оборудване, които командированите служители могат да използват по време на операцията в съответствие с Решение 2008/615/ПВР;

к) логистичните условия по отношение на транспорта, настаняването и сигурността;

л) разпределението на разходите по съвместната операция, ако то се различава от предвиденото в член 34, първо изречение от Решение 2008/615/ПВР;

м) възможни други необходими елементи.

4. Декларациите, процедурите и определянията, предвидени в настоящия член, се възпроизвеждат в наръчника, посочен в член 18, параграф 2.

ГЛАВА 7

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 18

Приложение и наръчник

1. Допълнителните подробности по отношение на техническото и административното изпълнение на Решение 2008/615/ПВР са установени в приложението към настоящото решение.

2. Генералният секретариат на Съвета изготвя и поддържа актуализиран наръчник, който съдържа главно фактическа информация, предоставена от държавите-членки чрез декларациите, направени съгласно Решение 2008/615/ПВР или настоящото решение, или чрез нотификации до генералния секретариат на Съвета. Наръчникът е във формата на документ на Съвета.

Член 19

Независими органи за защита на данните

В съответствие с член 18, параграф 2 от настоящото решение държавите-членки информират генералния секретариат на Съвета относно независимите органи за защита на данните или съдебните органи, посочени в член 30, параграф 5 от Решение 2008/615/ПВР.

Член 20

Подготовка на решенията, както е посочено в член 25, параграф 2 от Решение 2008/615/ПВР

1. Съветът взема решение съгласно посоченото в член 25, параграф 2 от Решение 2008/615/ПВР въз основа на доклад за оценка, който се изготвя на основата на въпросник.

2. По отношение на автоматизирания обмен на данни в съответствие с глава 2 от Решение 2008/615/ПВР, докладът за оценка се основава също на посещение за оценка и на пилотно изпитване, които се извършват, когато съответната държава-членка е информирала генералния секретариат в съответствие с член 36, параграф 2, първо изречение от Решение 2008/615/ПВР.

3. Допълнителните подробности по процедурата са установени в глава 4 от приложението към настоящото решение.

Член 21

Оценка на обмена на данни

1. Редовно се извършва оценка на административното, техническото и финансовото прилагане на обмена на данни съгласно глава 2 от Решение 2008/615/ПВР, и по-специално на използването на механизма по член 15, параграф 5. Оценката се отнася до онези държави-членки, които към момента на оценяване вече прилагат Решение 2008/615/ПВР, и се извършва по отношение на категориите данни, за които вече е започнал

обмен между заинтересованите държави-членки. Оценката се основава на доклади от съответните държави-членки.

2. Допълнителните подробности по процедурата са установени в глава 4 от приложението към настоящото решение.

Член 22

Връзка със споразумението за изпълнение на Договора от Прюм

За държавите-членки, обвързани от Договора от Прюм, съответните разпоредби на настоящото решение и приложението към него, след пълното им изпълнение, се прилагат вместо съответстващите им разпоредби, съдържащи се в споразумението за изпълнение на Договора от Прюм. Всички други разпоредби от споразумението за изпълнение остават приложими между договарящите страни по Договора от Прюм.

Член 23

Изпълнение

Държавите-членки вземат необходимите мерки, за да спазят разпоредбите на настоящото решение в сроковете, посочени в член 36, параграф 1 от Решение 2008/615/ПВР.

Член 24

Прилагане

Настоящото решение поражда действие двадесет дни след публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Люксембург на 23 юни 2008 година.

За Съвета

Председател

I. JARC

ПРИЛОЖЕНИЕ

СЪДЪРЖАНИЕ

9.3. *Символни кодове*

9.4. *Кратко описание на транзакция*

9.5. *Дефиниции на запис тип-1*

9.6. *Дефиниции на запис тип-2*

9.7. *Кодове за компресия в сивата скала*

9.8. *Спецификация на съобщенията*

ГЛАВА 3: **Обмен на данни за регистрацията на превозни средства**

1. ***Общ набор от данни за автоматизирано търсене на данни за регистрацията на превозни средства***

1.1. *Определения*

1.2. *Търсене на превозно средство/собственик/ползвател*

2. ***Сигурност на данните***

2.1. *Обзорен преглед*

2.2. *Характеристики на сигурността, свързани с обмена на съобщения*

2.3. *Характеристики на сигурността, несвързани с обмена на съобщения*

3. ***Технически условия на обмена на данните***

3.1. *Общо описание на приложението EUCARIS*

3.2. *Функционални и нефункционални изисквания*

ГЛАВА 4: **Оценяване**

1. ***Процедура за оценяване съгласно член 20 (подготовка на решения в съответствие с член 25, параграф 2 от Решение 2008/615/ПВР)***

1.1. *Въпросник*

1.2. *Пилотно изпитване*

1.3. *Посещение за оценка*

1.4. *Докладване на Съвета*

2. ***Процедура за оценяване съгласно член 21***

2.1. *Статистика и доклад*

2.2. *Преразглеждане*

3. ***Експертни заседания***

ГЛАВА 1: **Обмен на ДНК данни**

1. ***Свързани с ДНК криминалистични въпроси, правила и алгоритми за сравняване***

1.1. *Свойства на ДНК профилите*

ДНК профилът може да съдържа 24 двойки числа, представляващи алелите на 24-те локуса, които също се използват в ДНК процедурите на Интерпол. Наименованията на тези локуси са показани в следната таблица:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

Седемте отбелязани в сиво локуса на най-горния ред представляват както настоящия европейски стандартен набор от локуси (ESS), така и стандартния набор на Интерпол от локуси (ISSOL).

Правила за включване:

ДНК профилите, до които държавите-членки предоставят достъп с цел търсене и сравняване, както и ДНК профилите, изпращани с цел търсене и сравняване, трябва да съдържат поне 6 изцяло обозначени ([1]) локуса, като могат да съдържат допълнителни локуси или непопълнени такива в зависимост от наличността им. Референтните ДНК профили трябва да съдържат поне 6 от седемте локуса на ESS. За да се повиши точността на съвпаденията, всички налични алели се съхраняват в индексираната база данни с ДНК профили и се използват за търсене и сравняване. Всяка държава-членка следва да приложи в най-краткия практически възможен срок всеки нов вариант на ESS от локуси, приет от ЕС.

Не се допускат смесени профили, така че алелните стойности на всеки локус ще се състоят само от 2 цифри, които могат да бъдат еднакви при наличие на хомозиготност в даден локус.

При заявка за търсене с неизвестна стойност „жокер“ („wild-cards“) или с микроварианти се спазват следните правила:

— всички нецифрови стойности, с изключение на амелогенина, съдържащи се в профила (напр. „o“, „f“, „r“, „na“, „nr“ или „un“), се превръщат автоматично при експортирането в „жокер“ (*) и се извършва пълно търсене,

— цифровите стойности 0, 1 или 99, съдържащи се в профила, се превръщат автоматично при експортирането в „жокер“ (*) и се извършва пълно търсене,

— ако за един локус са подадени 3 алела, приема се първият алел, а останалите 2 алела се превръщат автоматично при експортирането в „жокер“ (*) и се извършва пълно търсене,

— когато за алел 1 или 2 е подадена стойност „жокер“ (*), се търсят и двете пермутации на цифровата стойност за локуса (напр. 12, * може да съответства на 12,14 или на 9,12),

— микровариантите на пентануклеотид (Penta D, Penta E и CD4) се сравняват по следния начин:

  x.1 = x, x.1, x.2

  x.2 = x.1, x.2, x.3

  x.3 = x.2, x.3, x.4

  x.4 = x.3, x.4, x + 1,

— микровариантите на тетрануклеотид (останалите локуси са тетрануклеотиди) се сравняват по следния начин:

  x.1 = x, x.1, x.2

  x.2 = x.1, x.2, x.3

  x.3 = x.2, x.3, x + 1

([1]) „Изцяло обозначени“ означава, че е включено обработването на редки алелни стойности.

1.2. *Правила за сравняване*

Сравняването на 2 ДНК профила се извършва въз основа на локусите, за които и в двата ДНК профила е налице една и съща алелна двойка. В двата ДНК профила трябва да има съвпадение на поне 6 изцяло обозначени локуса (без амелогенин), преди да се изпрати отговор за наличие на съвпадение.

Пълно съвпадение (качество 1) се определя като съвпадение, когато са еднакви всички алелни стойности на сравняваните локуси, обикновено съдържащи се в искането и отговора на справка за ДНК профили. Близко съвпадение се определя като съвпадение, при което е налице различна стойност само за една от всичките сравнявани алели в двата ДНК профила (качества 2, 3 и 4). Приема се, че има близко съвпадение, само ако в двата сравнявани ДНК профила е налице съвпадение на поне 6 изцяло обозначени локуса.

Причините за близко съвпадение могат да бъдат следните:

— печатна грешка, допусната при ръчно въвеждане на данните за един от ДНК профилите в искането за справка или в ДНК базата данни,

— грешка при определянето или „извикването“ на алели в хода на процедурата за генериране на ДНК профила.

1.3. *Правила за съобщаване на резултатите*

Съобщават се както пълните, така и близките съвпадения и липсата на съвпадение.

Съобщението за резултатите се изпраща на националната точка за контакт, отправила искането, като се предоставя на разположение и на националната точка за контакт, до която е отправено искането (за да може тя да прецени естеството и броя на евентуалните следващи искания за допълнителни налични лични данни и друга информация, която е свързана с ДНК профила, съответстващ на съвпадението в съответствие с членове 5 и 10 от Решение 2008/615/ПВР).

2. ***Таблица на кодовите номера на държавите-членки***

В съответствие с Решение 2008/615/ПВР за определяне на наименованията на домейни, както и за другите конфигуративни параметри, които се изискват от приложенията за обмен на ДНК данни по защитени мрежи съгласно договореностите от Прюм, се използва кодиране по стандарта ISO 3166-1 alpha-2.

Кодовете по ISO 3166-1 alpha-2 са следните двубуквени кодове за държавите-членки.

Имена на държавите-членки	Код	Имена на държавите-членки	Код
Белгия	BE	Люксембург	LU
България	BG	Унгария	HU
Чешката република	CZ	Малта	MT
Дания	DK	Нидерландия	NL
Германия	DE	Австрия	AT
Естония	EE	Полша	PL
Гърция	EL	Португалия	PT
Испания	ES	Румъния	RO
Франция	FR	Словакия	SK
Ирландия	IE	Словения	SI
Италия	IT	Финландия	FI
Кипър	CY	Швеция	SE
Латвия	LV	Обединеното кралство	UK
Литва	LT		

3. ***Функционален анализ***

3.1. *Наличност на системата*

Исканията по член 3 от Решение 2008/615/ПВР следва да пристигат в съответната база данни по хронологичен ред съгласно реда им на изпращане, а отговорите следва да се изпращат така че да пристигат в поискалата ги държава-членка в 15-минутен срок от пристигането на искането.

3.2. *Втори етап*

Когато държава-членка получи съобщение за съвпадение, нейната национална точка за контакт отговаря за сравняването на стойностите на профила, предаден като запитване, и стойностите на профила(ите), получени като отговор, за да валидира и провери доказателствената стойност на профила. Националните точки за контакт могат да осъществяват пряк контакт помежду си с цел валидиране.

Процедурите за правна помощ започват след валидирането на съществуващо съвпадение между два профила, въз основа на получените по време на фазата за автоматизирано консултиране съобщения за „пълно съвпадение“ и „близко съвпадение“.

4. ***Документ за контрол на интерфейса при обмен на ДНК данни***

4.1. *Въведение*

4.1.1. Цели

В тази глава се определят изискванията за обмена на информация за ДНК профили между системите от ДНК бази данни на всички държави-членки. Полетата в заглавната част са дефинирани специално за целите на обмена на ДНК данни по линия на Прюм, а съдържащата данните част е разработена на базата на частта за данните за ДНК профили в XML-схемата, дефинирана за електронния портал на Интерпол за обмен на ДНК данни.

Данните се обменят чрез SMTP (Simple Mail Transfer Protocol) и други модерни технологии, като се използва сървър за централизирано предаване на съобщенията, предоставен от доставчика на мрежови услуги. XML-файлът се транспортира в съдържателната част на съобщението.

4.1.2. Обхват

Този ICD определя само съдържанието на съобщението. Всички специфични за мрежата и съобщението въпроси, се дефинират еднообразно, за да се осигури обща техническа база за обмен на ДНК данни.

Това включва:

— форма́та на полето „предмет“ на съобщението, за да може да се осъществи автоматизираната обработка на съобщенията,

— дали е необходимо да се криптира съдържанието и ако е така, кои методи следва да се изберат,

— максималната дължина на съобщението.

4.1.3. XML-структура и принципи

Съобщението във XML-формат е структурирано в:

— заглавна част, в която се съдържа информация относно параметрите на предаване и

— част за данните, в която се съдържа специфична информация за профила, както и самият профил.

За исканията и за отговорите се използва една и съща XML-схема.

За да могат да се правят изчерпателни проверки на неидентифицирани ДНК профили (член 4 от Решение 2008/615/ПВР), е възможно да се изпращат по няколко профила в едно съобщение. Максималният брой на профилите в едно съобщение трябва да бъде определен. Броят им зависи от максималния допустим размер на съобщенията и се определя след избора на пощенски сървър.

XML пример:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

(…)

</header>

<datas>

(…)

</datas>

[<datas> структурата на данните се повтаря, когато се изпращат повече профили (….) в едно SMTP-съобщение, разрешено само за случаите по член 4

</datas>]

</PRUEMDNA>

4.2. *Дефиниране на XML-структурата*

Следните дефиниции са само за целите на документирането и по-добрата четивност, а информацията със задължителен характер се дава във файла с XML-схема (PRUEM DNA.xsd).

4.2.1. Схема PRUEMDNAx (Schema PRUEMDNAx)

Тази схема съдържа следните полета:

Fields	Type	Description
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 … 500

4.2.2. Съдържание на заглавната структура

4.2.2.1. Заглавна част PRUEM (PRUEM header)

Тази структура описва заглавната част на XML-файла. Тя съдържа следните полета:

Fields	Type	Description
direction	PRUEM_header_dir	Direction of message flow
ref	String	Reference of the XML file
generator	String	Generator of XML file
schema_version	String	Version number of schema to use
requesting	PRUEM_header_info	Requesting Member State info
requested	PRUEM_header_info	Requested Member State info

4.2.2.2. PRUEM_header dir

Тип данни, съдържащи се в съобщението — възможни стойности:

Value	Description
R	Request

Value	Description
A	Answer

4.2.2.3. PRUEM header info

Структура, описваща държавата-членка и датата/часа на съобщението. Съдържа следните полета:

Fields	Type	Description
source_isocode	String	ISO 3166-2 code of the requesting Member State
destination_isocode	String	ISO 3166-2 code of the requested Member State
request_id	String	unique Identifier for a request
date	Date	Date of creation of message
time	Time	Time of creation of message

4.2.3. Съдържание на данните за профили по линия на Прюм (PRUEM Profile data)

4.2.3.1. Данни по линия на Прюм (PRUEM_datas)

Тази структура описва частта за данни за профила на XML-файла. Съдържа следните полета:

Fields	Type	Description
reqtype	PRUEM request type	Type of request (Article 3 or 4)
date	Date	Date profile stored
type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of request
agency	String	Name of corresponding unit responsible for the profile
profile_ident	String	Unique Member State profile ID
message	String	Error Message, if result = E
profile	IPSG_DNA_profile	If direction = A (Answer) AND result ≠ H (Hit) empty
match_id	String	In case of a HIT PROFILE_ID of the requesting profile
quality	PRUEM_hitquality_type	Quality of Hit
hitcount	Integer	Count of matched Alleles
rescount	Integer	Count of matched profiles. If direction = R (Request), then empty. If quality! = 0 (the original requested profile), then empty.

4.2.3.2. Тип искане по линия на Прюм (PRUEM_request_type)

Тип данни, съдържащи се в съобщението — възможни стойности:

Value	Description
3	Requests pursuant to Article 3 of Decision 2008/615/JHA
4	Requests pursuant to Article 4 of Decision 2008/615/JHA

4.2.3.3. Тип качество на съвпадения по линия на Прюм (PRUEM_hitquality_type)

Value	Description
0	Referring original requesting profile: Case „No Hit“: original requesting profile sent back only; Case „Hit“: original requesting profile and matched profiles sent back.
1	Equal in all available alleles without wildcards
2	Equal in all available alleles with wildcards
3	Hit with Deviation (Microvariant)
4	Hit with mismatch

4.2.3.4. Тип данни по линия на Прюм (PRUEM_data_type)

Тип данни, съдържащи се в съобщението — възможни стойности:

Value	Description
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

Тип данни, съдържащи се в съобщението — възможни стойности:

Value	Description
U	Undefined, If direction = R (request)
H	Hit
N	No Hit
E	Error

4.2.3.6. IPSG_DNA_profile

Структура, описваща ДНК профил. Съдържа следните полета:

Fields	Type	Description
ess_issol	IPSG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSG_DNA_additional_loci	Other loci
marker	String	Method used to generate of DNA
profile_id	String	Unique identifier for DNA profile

4.2.3.7. IPSG_DNA_ISSOL

Структура, съдържаща локусите на ISSOL (стандартния набор на Интерпол от локуси). Съдържа следните полета:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Fields	Type	Description
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogin

4.2.3.8. IPSG_DNA_additional_loci

Структура, съдържаща другите локуси. Съдържа следните полета:

Fields	Type	Description
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317
d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9. IPSG_DNA_locus

Структура, описваща локус. Съдържа следните полета:

Fields	Type	Description
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. *Архитектура на приложението, сигурността и комуникациите*

5.1. *Обзорен преглед*

При внедряването на приложенията за обмен на ДНК данни в рамките на Решение 2008/615/ПВР се използва обща комуникационна мрежа, която е логически затворена между държавите-членки. С цел експлоатиране по по-ефективен начин на тази обща комуникационна инфраструктура за изпращане на искания и получаване на

отговори се възприема асинхронен механизъм за предаване на исканията за ДНК данни и дактилоскопични данни в капсулирани SMTP-електронни съобщения. С цел да се удовлетворят изискванията за сигурност, като разширение на SMTP-функционалността ще се използва механизъм sMIME, за да се установи действително затворен сигурен „тунел“ за работата в мрежата.

Оперативната TESTA (трансевропейски телематични услуги между администрациите) се използва за комуникационна мрежа за обмена на данни между държавите-членки. TESTA се управлява от Европейската комисия. С оглед на факта, че националните ДНК бази данни и действащите национални точки за достъп до TESTA могат да бъдат разположени на различни места в държавите-членки, достъпът до TESTA може да се осигури, като:

1. се използват съществуващите национални точки за достъп или се създаде нова национална точка за достъп до TESTA; или

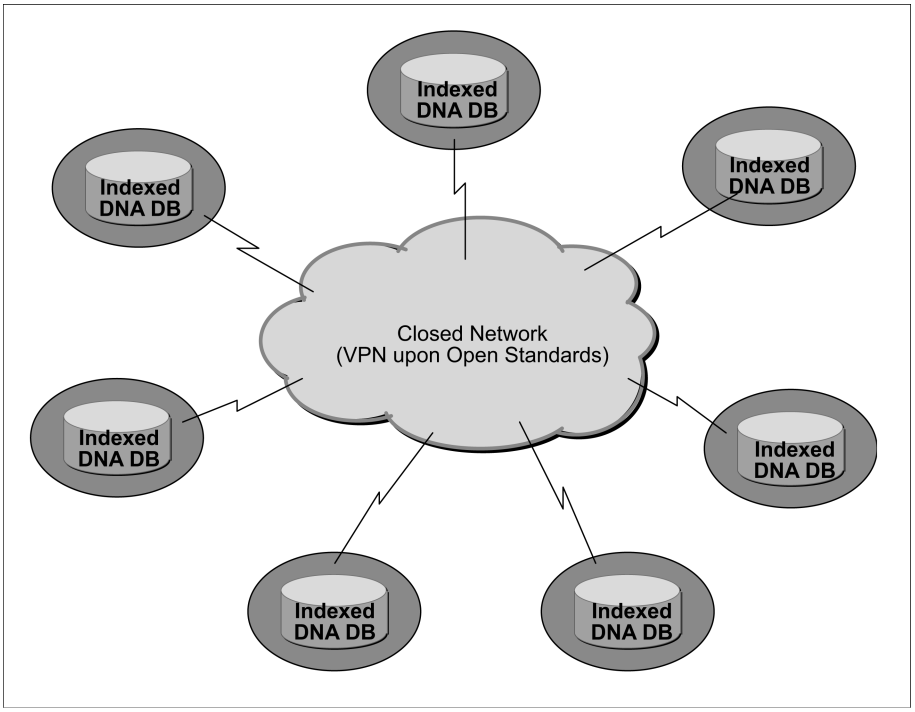
2. се създаде защитена местна връзка от обекта, където е разположена ДНК базата данни, управлявана от компетентната национална служба, до съществуващата национална точка за достъп до TESTA.

Протоколите и стандартите, внедрени в приложенията, използвани за изпълнението на Решение 2008/615/ПВР, съответстват на отворените стандарти и отговарят на изискванията, наложени от органите, определящи националната политиката по отношение на сигурността в държавите-членки.

5.2. *Архитектура на горното ниво*

В обхвата на Решение 2008/615/ПВР всяка държава-членка ще прави налични нейните ДНК данни за целите на обмена на такива данни и/или търсения в тях от други държави-членки в съответствие със стандартизирания общ формат на данните. Архитектурата е снована на комуникационен модел, при който се осъществява връзка „от всеки до всеки“. Не съществува централен компютърен сървър, нито централизирана база данни за съхранение на ДНК профили.

Фигура 1: Топология на облена на ДНК данни



Освен спазването на националните правни ограничения, касаещи съответните обекти в държавите-членки, всяка държава-членка може да реши какъв вид хардуер и софтуер следва да се внедри за конфигуриране в съответния обект, така че да са спазени изискванията на Решение 2008/615/ПВР.

5.3. *Стандарти за сигурност и защита на данните*

Три са нивата на сигурност, които са взети под внимание и са въведени.

5.3.1. На ниво данни

Предоставяните от държавите-членки данни за ДНК профили трябва да се изготвят в съответствие с общите стандарти за защита на данните, така че отправилата искането държава-членка да получи отговор, в който основно се посочва наличие на попадение или липса на попадение (HIT/NO-HIT) заедно с идентификационен номер в случай на попадение, но в него не се съдържа никаква лична информация. По-нататъшното разследване след уведомяване за наличие на попадение се води на двустранно равнище съгласно съществуващите национални правни и организационни разпоредби, уреждащи съответните обекти в държавите-членки.

5.3.2. На ниво комуникация

Съобщенията, съдържащи информация за ДНК профили (искания и отговори), се криптират посредством най-модерен механизъм в съответствие с отворените стандарти, като sMIME, преди да се изпратят в съответните обекти в държавите-членки.

5.3.3. На ниво предаване

Всички криптирани съобщения, съдържащи информация за ДНК профили, се изпращат в обектите на другите държави-членки посредством виртуална частна тунелираща система администрирана от надежден доставчик на мрежови услуги на национално равнище и връзките за сигурност към тази тунелираща система са под национално управление. Виртуалната частна тунелираща система няма никакъв точка на контакт с откритата интернет мрежа.

5.4. *Протоколи и стандарти, които да се използват за механизма за криптиране sMIME и свързани пакети*

Отвореният стандарт sMIME, като разширение на действащия *de facto* стандарт за електронна поща SMTP, ще се внедри за криптиране на съобщения, съдържащи информация за ДНК профили. Протоколът sMIME (V3) позволява електронно подписана разписка, етикети за сигурност и защитени списъци с електронни адреси (mailing lists), като е базиран върху „пласта“ на Cryptographic Message Syntax (CMS), IETF спецификация за защитени чрез криптиране съобщения. Той може да се използва за електронно подписване, резюмиране, автентификация или криптиране на всякакви форма цифрови данни.

Сертификатът, на базата на който се прилага механизмът sMIME, трябва да съответства на стандарта X.509. С цел да се осигурят стандарти и процедури, които са общи с тези за други приложения, използвани по линия на Прюм, правилата за обработване за операциите по криптиране на базата на sMIME или за прилагане в различни видове среда на базата на готови търговски продукти (Commercial Product of the Shelves — COTS), са следните:

— последователността на операциите е: първо криптиране и след това подписване,

— за симетрично и асиметрично криптиране се прилагат съответно алгоритмите за криптиране AES (Advanced Encryption Standard) с 256-битов ключ и RSA с 1 024-битов ключ,

— прилага се hash-алгоритъм SHA-1.

Функционалността s/MIME е вградена в повечето съвременни софтуерни пакети за електронна поща, в т.ч. Outlook, Mozilla Mail и Netscape Communicator 4.x, като позволява оперативна съвместимост между повечето основни софтуерни пакети за електронна поща.

Поради лесното интегриране на sMIME в националната ИТ инфраструктура във всички държави-членки, този механизъм е избран като подходящ с цел осигуряване на сигурността на ниво комуникации. С цел по-ефикасен „тест на концепцията“ („Proof of Concept“) и намаляване на разходите обаче е избран стандартът JavaMail API, с който да се извърши прототипирането на обмена на ДНК данни. JavaMail API предоставя елементарно криптиране и декриптиране на електронни съобщения посредством s/MIME и/или OpenPGP. Целта е да се осигури прост и лесен за употреба програмно-приложен интерфейс (API) за клиентите на електронна поща, които желаят да изпращат и получават криптирани електронни съобщения в един от двата най-популярни формата за криптиране на електронни съобщения. Следователно, за да са изпълнени изискванията на Решение 2008/615/ПВР, ще е достатъчно високотехнологично внедряване на базата на JavaMail API, като например продуктът на Bouncy Castle JCE (Java Cryptographic Extension), който ще се използва за въвеждането на sMIME за прототипирането на обмена на ДНК данни между държавите-членки.

5.5. *Архитектура на приложението*

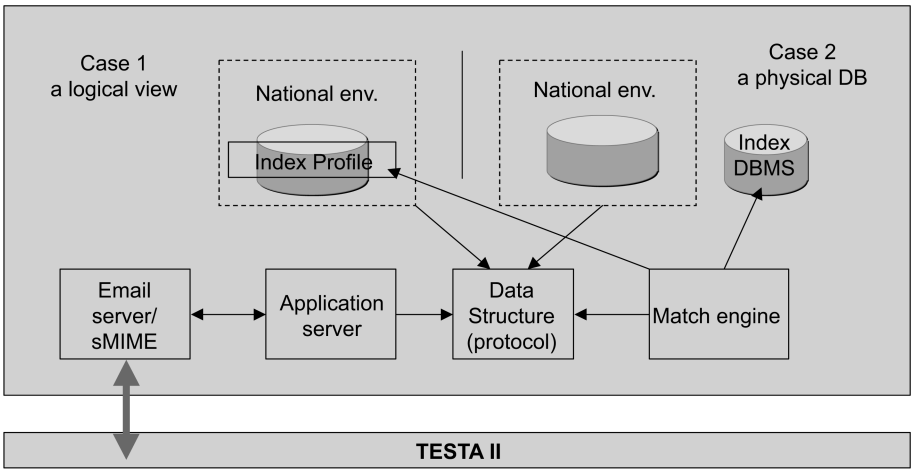
Всяка държава-членка ще предостави на другите държави-членки набор от стандартизирани данни за ДНК профили, които съответстват на използвания в момента общ документ за контрол на интерфейса (ICD). Това може да стане или чрез предоставяне на логически поглед върху индивидуалната национална база данни, или чрез установяване на физически експортирана база данни (индексирана база данни).

Четирите основни компонента: сървърът за електронна поща/sMIME, сървърът за приложението, зоната на структурирани данни (Data Structure Area) за извличане/подаване на данни и регистрация на входящите/изходящите съобщения, както и търсачката за сравняване, внедряват цялостната логика на приложението по начин, който не зависи от конкретните продукти.

За да се осигури на всички държави-членки възможност да интегрират лесно тези компоненти в съответните си национални обекти, конкретно определената обща функционалност е внедрена посредством компоненти с отворен код, които могат да се избират от всяка държава-членка в зависимост от нейната национална политика и уредба в областта на ИТ. Поради независимите характеристики на внедряваната система за получаване на достъп до индексирани бази данни с ДНК профили, обхванати от Решение 2008/615/ПВР, всяка държава-членка може свободно да избира собствената си хардуерна и софтуерна платформа, включително системите за бази данни и операционните системи.

Прототипът за обмена на ДНК данни е разработен и успешно изпитан в съществуващата обща мрежа. Вариант 1.0 е внедрен в работната среда и се използва за ежедневната дейност. Държавите-членки могат да използват разработения съвместно продукт, но също така могат да разработят свои продукти. Компонентите на общия продукт ще се поддържат, приспособяват и доразвиват в съответствие с изменящите се изисквания за функционалност по отношение на ИТ, криминалистиката и/или полицейската работа.

Фигура 2: Обща топология на приложението



5.6. *Протоколи и стандарти, които да се използват за архитектурата на приложението*

5.6.1. XML

Обменът на ДНК данни ще използва изцяло XML-схемата като ги прикачва към SMTP-електронни съобщения. Езикът XML (eXtensible Markup Language) се препоръчва от консорциума World Wide Web (W3C) като общофункционален метаезик за създаване на специализирани метаезици, способни да описват множество различни видове данни. Описанието на ДНК профила, който е подходящ за обмен между всички държави-членки, е изготвено посредством XML и XML-схема в ICD.

5.6.2. ODBC

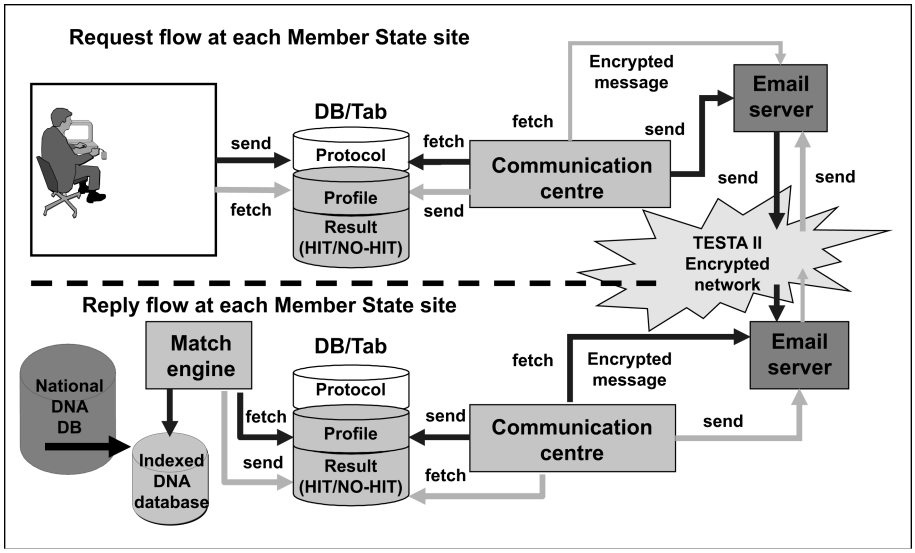
ODBC (Open DataBase Connectivity) предоставя стандартен софтуерен API метод за достъп до системи за управление на бази данни, който е независим от езиците за програмиране, от системите за базите данни и операционните системи. ODBC обаче си има своите недостатъци. Администрирането на голям брой клиентски машини може да е свързано с разнообразие на драйверите и DLL файловете. Това усложнение може да повиши разходите за администриране на системата.

5.6.3. JDBC

JDBC (Java DataBase Connectivity) представлява API за програмния език Java, който определя какъв достъп има клиентът до базата данни. За разлика от работата с ODBC, при JDBC не се изисква да се използва даден набор от местни DLL файлове на десктопа.

Работната логика на обработката на искания и отговори за ДНК профили в съответния обект на всяка държава-членка е описана в дадената по-долу диаграма. Потоците на исканията и на отговорите взаимодействат с неутрална зона за данни, която обхваща различни масиви с еднакво структурирани данни.

Фигура 3: Обща картина на работните потоци в приложенията в съответния обект на всяка държава-членка



5.7. *Комуникационна среда*

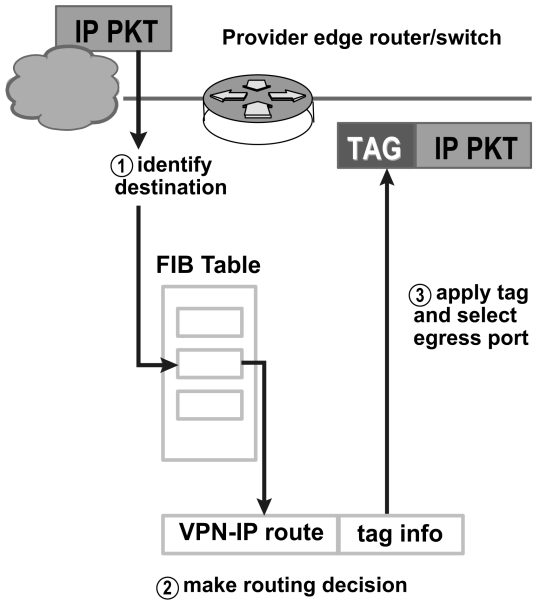
5.7.1. Обща комуникационна мрежа: TESTA и нейната последваща инфраструктура

Приложението за обмен на ДНК данни ще използва електронната поща, асинхронен механизъм, за изпращане на искания и получаване на отговори между държавите-членки. Тъй като всички държави-членки разполагат с поне една точка за достъп до мрежата TESTA, обменът на ДНК данни ще се осъществява по мрежата TESTA. TESTA осигурява редица услуги с добавена стойност посредством своята система за предаване на електронна поща. Освен хостването на специално предназначени за TESTA електронни пощенски кутии, инфраструктурата може да работи със списъци за разпределяне на съобщения и политики за маршрутизиране. Това позволява TESTA да се използва като разпределителен център за съобщенията, адресирани до администрациите, свързани с домейните в рамките на ЕС. Възможно е също така да се включат и механизми за проверка за вируси.

Системата на TESTA за предаване на електронна поща е изградена на базата на хардуерна платформа с висока степен на наличност, която е разположена в централното приложение на TESTA и е защитена с firewall. Чрез DNS (Domain Name Services) на TESTA ще се определят ресурсните локатори за IP-адресите и ще се скрива информацията по адресирането от потребителя и от приложението.

5.7.2. Обезпечаване на сигурността

В рамките на TESTA е приложена концепцията за VPN (Virtual Private Network). Технологията за Tag Switching, която е използвана за изграждане на тази VPN ще бъде доразвита, така че да поддържа стандарта MPLS (Multi-Protocol Label Switching), разработен от IETF (Internet Engineering Task Force).



MPLS представлява стандартна технология на IETF, която ускорява мрежовия трафик, като избягва пакетния анализ посредством междинни рутери („hops“). Това се прави на базата на т.нар. „етикети“, които се прикрепват към пакета от edge-рутерите в backbone въз основа на информацията, съхранена в информационната база за препращане (FIB). Етикети се използват и за внедряване на виртуалните частни мрежи (VPN).

В MPLS се съчетават ползите от маршрутизирането в пласт 3 с предимствата на суичинга в пласт 2. Тъй като на IP-адресите не се прави оценка при преминаването им през т.нар. „backbone“, MPLS не налага никакви ограничения на IP-адресирането.

Освен това електронните съобщения, предавани по TESTA, ще бъдат защитени с механизъм за криптиране на базата на sMIME. Никой не може да декриптира съобщенията по мрежата, ако не знае ключа и не разполага със съответния сертификат.

5.7.3. Протоколи и стандарти, които да се използват в комуникационната мрежа

5.7.3.1. SMTP

SMTP (Simple Mail Transfer Protocol) е действащият стандарт за пренос на електронна поща по Интернет. SMTP е относително прост текстови протокол, при който се определя един или повече получатели на съобщението, след което то се изпраща. SMTP използва TCP порт 25 по спецификациите на IETF. За да се определи SMTP сървърът за дадено име на домейн, се използва записване по MX (Mail eXchange) DNS (Domain Name Systems).

Тъй като този протокол отначало беше изцяло и само текстови на базата на ASCII, той не работеше добре с бинарни файлове. Стандарти като MIME бяха разработени, за да се кодират бинарни файлове за изпращане чрез SMTP. Днес повечето SMTP сървъри поддържат 8BITMIME и sMIME разширения, позволявайки изпращането на бинарни файлове да става почти толкова лесно, колкото и обикновен текст. Правилата за работа при операции с sMIME са описани в раздела „sMIME“ (вж. точка 5.4).

SMTP представлява push-протокол, който не позволява изтегляне на съобщения от физически отдалечен сървър по заявка. За да изтегли съобщение, клиентът на електронна поща трябва да използва POP3 или IMAP. За осъществяването на обмен на ДНК данни е решено да се използва POP3 протокол.

5.7.3.2. POP

Местните клиенти за електронна поща използват POP3 (Post Office Protocol version 3), протокол за интернет стандарт за пласта на приложението (application-layer Internet standard protocol), за да извлекат електронното съобщение от физически отдалечен сървър по TCP/IP връзка. Като използва профила SMTP Submit на SMTP протокола, клиентът на електронна поща изпраща съобщения по интернет или по корпоративна мрежа. MIME служи за стандарт за прикрепени файлове и текст, който не е ASCII, в електронното съобщение. Въпреки че нито POP3, нито SMTP изискват електронното съобщение да е в MIME-формат, предаваните по интернет електронни съобщения са основно в MIME-формат, така че POP-клиентите трябва също така да разбират и да използват MIME. Поради това в цялата комуникационна среда на Решение 2008/615/ПВР ще бъдат включени компонентите на POP.

5.7.4. Определяне на интернет адреси

Операционна среда

Понастоящем Европейският орган за регистрация на IP-адреси (RIPE) е определил за TESTA един специализиран блок от подмрежа клас C. По-нататък, ако е необходимо, за TESTA могат да бъдат определени и други блокове за адреси. Определянето на IP-адреси за държавите-членки се основава на географска схема в Европа. Обменът на данни между държавите-членки в рамките на Решение 2008/615/ПВР се осъществява по логически затворената европейска IP-мрежа.

Изпитателна среда

С цел да се осигури среда за безпрепятствено осъществяване на ежедневната работа между всички свързани държави-членки, е необходимо да се установи изпитателна среда в защитената мрежа за новите държави-членки, които се готвят да се присъединят към тези операции. Изготвен е документ с параметрите, включително IP-адреси, мрежови настройки, домейни за електронна поща, както и потребителски акаунти за приложенията, които следва да се конкретизират и установят в съответните обекти на държавите-членки. Освен това за целите на изпитванията е конструиран масив от псевдо ДНК профили.

5.7.5. Параметри на конфигурацията

Създадена е защитена мрежа за електронна поща, за което е използван домейнът eu-admin.net. Този домейн с асоциираните му адреси няма да бъде достъпен от места извън домейна на TESTA за ЕС, тъй като имената са известни само на централния DNS-сървър на TESTA, който е отделен от интернет със специална защита.

Превръщането на тези адреси на сайтове (host names) в TESTA в съответните им IP-адреси се осъществява от DNS-услугите на TESTA. В този централен DNS-сървър на TESTA се добавя вписване за пощата, като всички електронни съобщения, изпратени до местните домейни на TESTA, се предават на центъра за предаване на поща на TESTA. Този център за предаване на поща на TESTA след това ги препраща към конкретния сървър за електронна поща на местния домейн, като се използват адресите за електронна поща на местния домейн. Чрез предаването на електронната поща по този начин, критична информация, която се съдържа в електронните съобщения, ще преминава само по европейската защитената мрежова инфраструктура, а не по незащитен интернет.

Необходимо е в обектите на всички държави-членки да се установят поддомейни (***получерен курсив***), следвайки следния синтаксис:

„application-type.pruem.Member State-code.eu-admin.net“, където:

„Member State-code“ приема стойността на един от двубуквените кодове на държавите-членки (напр. AT, BE и т.н.).

„***application-type***“ приема една от стойностите: DNA или FP.

Като се приложи горепосоченият синтаксис, поддомейните на държавите-членки са посочени в таблицата по-долу:

MS	Sub Domains	Comments
BE	***dna*.pruem.be**.eu-admin.net	Setting up a secure local link to the existing TESTA II access point
	***fp*.pruem.be**.eu-admin.net	
BG	***dna*.pruem.bg**.eu-admin.net	
	***fp*.pruem.bg**.eu-admin.net	
CZ	***dna*.pruem.cz**.eu-admin.net	
	***fp*.pruem.cz**.eu-admin.net	
DK	***dna*.pruem.dk**.eu-admin.net	
	***fp*.pruem.dk**.eu-admin.net	
DE	***dna*.pruem.de**.eu-admin.net	Using the existing TESTA II national access points
	***fp*.pruem.de**.eu-admin.net	
EE	***dna*.pruem.ee**.eu-admin.net	
	***fp*.pruem.ee**.eu-admin.net	

MS	Sub Domains	Comments
IE	***dna*.pruem.ie**.eu-admin.net	
	***fp*.pruem.ie**.eu-admin.net	
EL	***dna*.pruem.el**.eu-admin.net	
	***fp*.pruem.el**.eu-admin.net	
ES	***dna*.pruem.es**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.es**.eu-admin.net	
FR	***dna*.pruem.fr**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.fr**.eu-admin.net	
IT	***dna*.pruem.it**.eu-admin.net	
	***fp*.pruem.it**.eu-admin.net	
CY	***dna*.pruem.cy**.eu-admin.net	
	***fp*.pruem.cy**.eu-admin.net	
LV	***dna*.pruem.lv**.eu-admin.net	
	***fp*.pruem.lv**.eu-admin.net	
LT	***dna*.pruem.lt**.eu-admin.net	
	***fp*.pruem.lt**.eu-admin.net	
LU	***dna*.pruem.lu**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.lu**.eu-admin.net	
HU	***dna*.pruem.hu**.eu-admin.net	
	***fp*.pruem.hu**.eu-admin.net	
MT	***dna*.pruem.mt**.eu-admin.net	
	***fp*.pruem.mt**.eu-admin.net	
NL	***dna*.pruem.nl**.eu-admin.net	Intending to establish a new TESTA II access point at the NFI
	***fp*.pruem.nl**.eu-admin.net	
AT	***dna*.pruem.at**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.at**.eu-admin.net	
PL	***dna*.pruem.pl**.eu-admin.net	
	***fp*.pruem.pl**.eu-admin.net	
PT	***dna*.pruem.pt**.eu-admin.net	.....
	***fp*.pruem.pt**.eu-admin.net	.....
RO	***dna*.pruem.ro**.eu-admin.net	
	***fp*.pruem.ro**.eu-admin.net	

MS	Sub Domains	Comments
SI	***dna*.pruem.si**.eu-admin.net	.....
	***fp*.pruem.si**.eu-admin.net	.....
SK	***dna*.pruem.sk**.eu-admin.net	
	***fp*.pruem.sk**.eu-admin.net	
FI	***dna*.pruem.fi**.eu-admin.net	[To be inserted]
	***fp*.pruem.fi**.eu-admin.net	
SE	***dna*.pruem.se**.eu-admin.net	
	***fp*.pruem.se**.eu-admin.net	
UK	***dna*.pruem.uk**.eu-admin.net	
	***fp*.pruem.uk**.eu-admin.net	

ГЛАВА 2: **Обмен на дактилоскопични данни (документ за контрол на интерфейса)**

Целта на следния документ за контрол на интерфейса е да определи изискванията за обмена на дактилоскопична информация между системите на държавите-членки за автоматизирана идентификация на пръстови отпечатъци (AFIS). Документът се основава на прилагания от Интерпол ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b).

Настоящата версия обхваща всички основни дефиниции за логически записи тип-1, тип-2, тип-4, тип-9, тип-13 и тип-15, които са необходими за обработката на дактилоскопични данни на базата на изображения и признаци (*minutiae*).

1. ***Обзор на съдържанието на файловете***

Дактилоскопичният файл се състои от няколко логически записа. В оригиналния стандарт ANSI/NIST-ITL 1-2000 са определени шестнадесет типа записи. За разделяне на записите и на техните полета и подполета се използват подходящи разделителни ASCII символи.

За обмен на информация между службата по произход и службата по местоназначението се използват само 6 типа записи:

Тип-1 → информация за транзакция

Тип-2 → буквено-цифрови данни за лица/случай

Тип-4 → дактилоскопични изображения с висока резолюция в сивата скала

Тип-9 → запис на признаци (*minutiae*)

Тип-13 → запис на изображение на следи с променлива резолюция

Тип-15 → запис на изображение на отпечатък от длан с променлива резолюция

1.1. *Тип-1 — заглавна част на файла*

Този запис съдържа маршрутизираща информация и информация, описваща структурата на останалата част от файла. В този тип записи също така се описват типовете транзакции, които попадат в следните по-широки категории:

1.2. *Тип-2 — описателен текст*

Този запис съдържа текстова информация, която е от интерес за изпращащата и получаващата служба.

1.3. *Тип-4 — изображение с висока резолюция в сивата скала*

Този запис се използва за обмен на дактилоскопични изображения с висока резолюция в сивата скала (осем бита), снети при резолюция 500 пиксела/инч. Дактилоскопичните изображения се компресират, като се използва WSQ-алгоритъм при съотношение не повече от 15:1. Не трябва да се използват други алгоритми за компресия или некомпресирани изображения.

1.4. *Тип-9 — запис на признаци (minutiae)*

Записите тип-9 се използват за обмен на характеристики на папиларните линии и данни за признаците. Тяхната цел е от една страна да се избегне ненужното дублиране на процесите за кодиране в AFIS, от друга — да се позволи изпращането на AFIS кодове, които съдържат по-малко информация отколкото съответните изображения.

1.5. *Type-13 — запис на изображение на следи с променлива резолюция*

Този запис се използва за обмен на изображения на следи от пръстови отпечатъци и на следи от длан с променлива резолюция, придружавани от буквено-цифрова текстурна информация. Резолюцията на сканиране на изображенията е 500 пиксела/инч с 256 нива на сивото. Ако качеството на изображението на следа е задоволително, то се компресира по WSQ алгоритъм. Ако е необходимо, на основата на двустранно споразумение, може резолюцията на изображенията да се увеличи на повече от 500 пиксела/инч и повече от 256 нива на сивото. В този случай е силно препоръчително да се използва JPEG 2000 (вж. допълнение 7).

1.6. *Запис на изображение на отпечатък от длан с променлива резолюция*

Записи тип-15 на изображения с маркировка на полетата се използват за обмен на изображения на отпечатък от длан с променлива резолюция, придружавани от буквено-цифрова текстурна информация. Резолюцията на сканиране на изображенията е 500 пиксела/инч с 256 нива на сивото. За да се намали максимално обемът на данните, всички изображения на отпечатък от длан се компресират като се използва WSQ алгоритъм. Ако е необходимо, на основата на двустранно споразумение, резолюцията на изображенията може да се увеличи на повече от 500 пиксела/инч и повече от 256 нива на сивото. В този случай е препоръчително да се използва JPEG 2000 (вж. допълнение 7).

2. ***Формат на записите***

Файлът за транзакция се състои от един или повече логически записа. За всеки логически запис, който се съдържа във файла, има по няколко информационни полета, подходящи за типа запис. Всяко информационно поле може да съдържа една или повече на брой информационни единици с единична стойност. Тези единици взети заедно се използват за предаване на различни аспекти на данните, които се съдържат в съответното поле. Информационното поле може да се състои също така от една или повече информационни единици, които са групирани и повторени неколкократно в рамките на полето. Групираните по този начин информационни единици са познати като подполе. Следователно, информационното поле може да се състои от едно или повече подполета от информационни единици.

2.1. *Информационни разделители*

В логическите записи с тагови полета, се прилагат механизми за отграничаване на информацията, посредством използването на четири ASCII разделителя. По този начин могат да се отграничават отделни единици в рамките на полето или подполето, полетата в рамките на логическия запис или многократно появяващи се подполета. Разделителите на информацията са дефинирани в стандарта ANSI X3.4. Тези символи се използват за логическо разделяне и категоризиране на информацията. Представени йерархично, символът за разделяне на файлове (FS) има най-широк обхват, следван от символа за разделяне на групи (GS), символа за разделяне на записи (RS) и накрая — символа за разделяне на единици (US). В таблица 1 са изброени тези ASCII разделители и е дадено описание на употребата им в настоящия стандарт.

Във функционално отношение информационните разделители следва да се разглеждат като указание за типа на данните, които следват. Със символ US се разделят отделни информационни единици в рамките на полето или подполето. Това е сигнал, че следващата информационна единица е част от данните за това поле или подполе. Множество подполета в рамките на същото поле, отделено със символ RS, сигнализира за започването на следваща група от повтаряща(и) се информационна(и) единица(и). Разделителният символ GS, използван между информационните полета, сигнализира за началото на ново поле, предшестващо идентификационния номер на полето, което се появява. По същия начин, началото на нов логически запис се сигнализира от появата на символа FS.

Четирите символа имат смисъл само когато са използвани като разделители на информационни единици в полетата на ASCII текстови записи. Когато тези символи се срещат в бинарни записи на изображения и бинарни полета не им се придава конкретен смисъл — те представляват част от обменяните данни.

Обикновено не следва да има празни полета или информационни единици, поради което между две единици данни следва да появява само един разделител. Изключение от това правило възниква в тези случаи, когато данните в полетата или информационните единици на транзакцията не са налични, липсват или не са задължителни и обработката на транзакцията не зависи от присъствието на точно тези данни. В тези случаи се появяват няколко и адаптиращи разделителни символа заедно, вместо да се изисква вмъкване на заместители на данни между разделителните символи.

За дефиниране на поле, което се състои от три информационни единици, се прилага следното: ако липсва информацията за втората информационна единица, тогава се появяват два съседни разделителя US между първата и третата информационна единица; ако липсват и втората и третата информационна единица, тогава се използват три разделителни символа — два символа US в допълнение към символа за край на полето или към разделителния символ на подполето. По принцип ако не са налични една или повече задължителни или незадължителни информационни единици в рамките на едно поле или подполе, следва да се постави съответният брой разделителни символи.

Възможно е да се получат съседни комбинации от два или повече от четирите вида разделителни символи. Когато отсъстват или не са налични данни за информационните единици, подполета или полета, трябва да има един разделителен символ по-малко, отколкото са задължителните информационни единици, подполета или полета.

Таблица 1: Използвани разделители

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2. *Изглед на записите*

При логическите записи с тагови полета всяко използвано информационно поле се номерира в съответствие с настоящия стандарт. Форматът за всяко поле се състои от номера на типа логически запис, следван на разстояние от точка „.“, номер на полето, следван от двоеточие „:“, след което подходяща информация за това поле. Таговото поле може да се номерира с всяка цифра от едно до девет, като номерът се повява между точката „.“ и двоеточието „:“. Интерпретира се като номер на поле с непълно изписване. Това означава, че номерът на поле „2123:“ е равностоен на номера на поле „2.000000123:“ и се интерпретира по същия начин.

С цел илюстрация в настоящия документ се използват трицифрени номера за номериране на полетата, които се съдържат във всеки от описаните тук логическите записи с тагови полета. Номерата на полетата са в следния формат: „TT.xxx:“ където „TT“ представлява еднозначен или двусимволен тип запис, следван от точка. Следващите три символа съставят съответния номер на полето, следван от двоеточие След двоеточието се намира описателната ASCII информация или данните на изображението.

Логическите записи тип-1 и тип-2 съдържат само полета с ASCII текст. Цялата дължина на записа (включително номерата на полета, двоеточията и разделителните символи) се записва като първо ASCII поле във всеки от посочените типове записи. Контролният ASCII символ за разделяне на файлове FS (който означава край на логическия запис или транзакция) се поставя след последния байт ASCII информация и се включва в дължината на записа.

За разлика от концепцията за таговите полета, запис тип-4 съдържа само бинарни данни, записани като поредица от бинарни полета с фиксирана дължина. Цялата дължина на записа се отразява в първото четирибайтово бинарно поле на съответния запис. За този бинарен запис не се отразява нито номер на записа със съответната точка в края, нито идентификационен номер на полето със съответното двоеточие. Освен това, тъй като всички дължини на полета на този тип запис са или фиксирани, или конкретно определени, никой от четирите разделителни символа (US, RS, GS или FS) не се интерпретира по друг начин освен като бинарни данни. За бинарния запис символът FS не се използва за разделяне на записите или като символ, завършващ транзакцията.

3. ***Логически запис тип-1: заглавна част на файла***

Този запис описва структурата на файла, типа на файла и друга важна информация. Наборът от символи, използвани за полета на тип-1 се състои единствено от 7-битов ANSI код за информационен обмен.

3.1. *Полета на логически запис тип-1:*

3.1.1. Поле 1.001: Дължина на логическия запис (Logical Record Length — LEN)

В това поле се съдържа общия брой байтове в целия логически запис тип-1. Полето започва с „1.001:“, следвано от дължината на целия запис, в т.ч. всички символи на всички полета заедно с информационните разделители.

3.1.2. Поле 1.002: Номер на версията (Version Number — VER)

За да е сигурно, че потребителите знаят коя е използваната версия на стандарта ANSI/NIST, в това четирибайтово поле се посочва номерът на версията на стандарта, който е приложен от софтуера или системата, генерирали този файл. Първите два байта посочват номера на основната версия, а вторите два — номера на подверсията. Например, оригиналният стандарт от 1986 г. се счита за първа версия и се означава с „0100“, докато сегашният стандарт ANSI/NIST-ITL 1-2000 е „0300“.

3.1.3. Поле 1.003: Съдържание на файла (File Content — CNT)

Това поле изброява всеки от записите във файла според типа и реда, в който записите се появяват в логическия файл. Състои се от едно или повече подполета, всяко от които на свой ред съдържа две информационни единици, описващи един от логическите записи в текущия файл. Подполетата се вписват по реда на записването и изпращането на записите.

Първата информационна единица в първото подполе е „1“, с което се отбелязва, че въпросния запис е тип-1. Той се следва от втора информационна единица, която съдържа числото на броя на останалите записи, които се съдържат във файла. Това число е равно на броя на останалите подполета на поле 1.003.

Всяко от останалите подполета се асоциира с един от записите във файла, а редът на изброяване на подполетата съответства на последователността на записите. Всяко подполе съдържа две информационни единици. Първата показва какъв тип е записът. Втората е символът за означаване на изображението (IDC) в записа. За разделяне на двете информационни единици се използва символът *US*.

3.1.4. Поле 1.004: Тип транзакция (Type of Transaction — TOT)

Това поле съдържа трибуквено мнемонично съчетание, с което се означава типът транзакция. Тези кодове могат да се различават кодовете, които се използват в други случаи на прилагане на стандарта ANSI/NIST.

CPS (Criminal Print-to-Print Search): търсене на отпечатъци на правонарушител. Тази транзакция представлява искане за търсене на запис, свързан с престъпление, чрез сравняване на отпечатъци в база данни. Отпечатъците на лицето трябва да се включат във файла като WSQ-компресирани изображения.

Ако не се установи попадение (No-HIT), се изпраща следният логически запис:

— 1 Type-1 Record

— 1 Type-2 Record

Ако се установи попадение (HIT), се изпраща следният логически запис:

— 1 Type-1 Record

— 1 Type-2 Record

— 1-14 Type-4 Record

В таблица A.6.1 (допълнение 6) е представен накратко TOT CPS.

PMS (Print-to-Latent Search): търсене чрез сравняване на отпечатъци със следи. Тази транзакция се използва, когато в база данни с неидентифицирани следи се извършва търсене за определен набор отпечатъци. В отговора се съдържа решението за наличие или отсъствие на попадение (Hit/No-Hit) при търсенето в AFIS по местоназначение. Ако има повече неидентифицирани следи, се отговаря с няколко SRE транзакции — по една отделна транзакция за всяка следа. Отпечатъците на лицето трябва да се включат във файла като WSQ-компресирани изображения.

Ако не се установи попадение (No-HIT), се изпраща следният логически запис:

— 1 Type-1 Record

— 1 Type-2 Record.

Ако се установи попадение (HIT), се изпраща следният логически запис:

— 1 Type-1 Record

— 1 Type-2 Record

— 1 Type-13 Record.

В таблица A.6.1 (допълнение 6) е представен накратко TOT PMS.

MPS (Print-to-Latent Search): търсене чрез сравняване на следи с отпечатъци. Тази транзакция се използва, когато трябва да се търсят съответствия на следи в база данни с отпечатъци. Във файла трябва да се включи информацията за признаците (*minutiae*) на следите и изображението (WSQ-компресия).

Ако не се установи попадение (No-HIT), се изпраща следният логически запис:

— 1 Type-1 Record,

— 1 Type-2 Record.

Ако се установи попадение (HIT), се изпраща следният логически запис:

— 1 Type-1 Record,

— 1 Type-2 Record,

— 1 Type-4 or Type-15 Record.

В таблица A.6.4 (допълнение 6) е представен накратко TOT MPS.

MMS (Latent-to-Latent Search): търсене чрез сравняване на следи със следи. При тази транзакция файлът съдържа следа, за която се прави търсене в база данни с неидентифицирани следи, за да се установи връзка между различни местопрестъпления. Във файла трябва да се включи информацията за признаците (*minutiae*) на следите и изображението (WSQ-компресия).

Ако не се установи попадение (No-HIT), се изпраща следният логически запис:

— 1 Type-1 Record,

— 1 Type-2 Record.

Ако се установи попадение (HIT), се изпраща следният логически запис:

— 1 Type-1 Record,

— 1 Type-2 Record,

— 1 Type-13 Record.

В таблица A.6.4 (допълнение 6) е представен накратко TOT MMS.

SRE: Тази транзакция се изпраща от службата по местоназначение в отговор на заявка с дактилоскопични данни. В отговора се съдържа решението за наличие или отсъствие на попадение (Hit/No-Hit) при търсенето в AFIS по местоназначение. Ако са налице няколко кандидати, се отговаря с няколко SRE транзакции — отделна транзакция за всеки кандидат.

В таблица A.6.2 (допълнение 6) е представен накратко TOT SRE.

ERR: тази транзакция се изпраща от AFIS по местоназначение, за да се посочи, че има грешка. В нея се включва поле за съобщение (ERM), в което се посочва установената грешка. Изпраща се следният логически запис:

— 1 Type-1 Record,

— 1 Type-2 Record.

В таблица A.6.3 (допълнение 6) е представен накратко TOT ERR.

Таблица 2: Допустими кодове в транзакциите

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SRE	M	M	C	— (C in case of latent hits)	C	C
MPS	M	M	—	M (1*)	M	—

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

Легенда:

M = задължително
M* = може да се включи само един от двата типа записи
O = незадължително
C = в зависимост от това, дали има налични данни
— = недопустимо
1* = в зависимост от това какви са „наследените“ системи

3.1.5. Поле 1.005: Дата на транзакцията (Date of Transaction — DAT)

В това поле се посочва датата, на която е започнала транзакцията, като се използва стандартният формат на ISO: YYYYMMDD

където YYYY е годината, MM е месецът, а DD е денят от месеца. Единичните цифри се предшестват от нула. Например „19931004“ означава 4 октомври 1993 г.

3.1.6. Поле 1.006: Приоритет (Priority — PRY)

Това незадължително поле описва приоритета на искането по скала от 1 до 9, като „1“ е най-високият приоритет, а „9“ е най-ниският. Транзакциите с приоритет „1“ се обработват незабавно.

3.1.7. Поле 1.007: Идентификатор на службата по местоназначение (Destination Agency Identifier — DAI)

В това поле се посочва службата по местоназначение на транзакцията.

Състои се от две информационни единици в следния формат: CC/*служба*.

Първата информационна единица съдържа кода на държавата, определен по ISO 3166, с дължина два буквено-цифрови символа. Втората единица, *службата*, представлява свободен текст за идентификация на службата — не повече от 32 буквено-цифрови символа.

3.1.8. Поле 1.008: Идентификатор на службата на произход (Originating Agency Identifier — ORI)

В това поле се посочва службата на произход и се използва същият формат като този за DAI (поле 1.007).

3.1.9. Поле 1.009: контролен номер на транзакцията (Transaction Control Number — TCN)

Това е контролен номер за справочни цели. Той следва да се генерира от компютъра и е в следния формат: YYSSSSSSSSA

където YY е годината на транзакцията, SSSSSSSS е 8-цифров сериен номер, а A е контролен символ, генериран по процедурата, описана в допълнение 2.

Където няма TCN, полето YYSSSSSSSS се запълва с нули и се генерира контролен символ по начина, описан по-горе.

3.1.10. Поле 1.010: Контролен номер на отговора на транзакцията (Transaction Control Response — TCR)

Когато има изпратено искане, на което настоящото се явява отговор, в това незадължително поле се дава контролният номер на транзакцията, с която е изпратено искането. Следователно, то има същия формат като TCN (поле 1.009).

3.1.11. Поле 1.011: Резолюция на сканирането на мястото на произход (Native Scanning Resolution — NSR)

В това поле се посочва нормалната резолюция на сканиране на системата, с която работи службата-подател на транзакцията. Резолюцията се посочва във формат на две числа, следвани от десетична точка и след това още две цифри.

Всички транзакции, осъществявани по силата на Решение 2008/615/ПВР, се подават във формат 500 пиксела/инч или 19,68 пиксела/mm.

3.1.12. Поле 1.012: Номинална резолюция на предаване (Nominal Transmitting Resolution — NTR)

В това 5-байтово поле се посочва номиналната резолюция на предаване на изпращаните изображения Резолюцията се изразява в пиксели/mm в същия формат като NSR (поле 1.011).

3.1.13. Поле 1.013: Наименование на домейн (Domain name — DOM)

В това незадължително поле се посочва наименованието на домейна за изпълнението на определения от потребителя логически запис тип-2. Състои се от две информационни единици и е „INT-I{US}4.22{GS}“.

3.1.14. Поле 1.014: Средно време по Гринуич (Greenwich mean time — GMT)

Това задължително поле предоставя механизъм за отразяване на датата и часа чрез универсалните единици в съответствие със средното време по Гринуич (GMT). Когато се използва полето GMT, в него се отразява тази универсална дата като допълнение към местната дата, дадена в поле 1.005 (DAT). С използването на полето GMT се премахват несъответствията в местното време, които се появяват, когато транзакцията и отговорът се предават между места, разделени от няколко часови зони. В полето GMT се посочва универсална дата и час в 24-часов формат, независимо от часовите зони. Изразява се във формат „CCYYMMDDHHMMSSZ“ — поредица от 15 символа, представляваща съчетанието от датата заедно с GMT и завършва със „Z“. Символите в поредицата „CCYY“ представляват годината на транзакцията, символите в поредицата „MM“ са стойностите на десетицата и единицата на месеца, а символите в поредицата „DD“ са стойностите на десетицата и единицата на деня от месеца, като символите в поредицата „HH“ представляват часа, „MM“ — минутата, а „SS“ — секундата. Пълната дата не може да има стойност по-висока от стойността на настоящата дата.

4. ***Логически запис тип-2: описателен текст***

Структурата на по-голямата част от този запис не е дефинирана в първоначалния стандарт ANSI/NIST. Записът съдържа информация, която представлява специален интерес за службите, които изпращат или получават файла. За да е сигурно, че съответните дактилоскопични системи, между които се осъществява комуникацията, са съвместими, в записа е необходимо да се включат само изброените по-долу полета. В документа се посочва кои полета са задължителни и кои не са задължителни, като се дефинира и структурата на отделните полета.

4.1. *Полета в логически запис тип-2:*

4.1.1. Поле 2.001: Дължина на логическия запис (Logical Record Length — LEN)

В това задължително поле се дава дължината на настоящия запис тип-2 и се посочва общият брой на байтовете, като се включват всички символи във всички полета на записа плюс разделителите.

4.1.2. Поле 2.002: Символ за означение на изображението (Image Designation Character — IDC)

Това задължително поле съдържа символа за обозначение на изображението (IDC), представен в ASCII-формат за съответния IDC, определен в съдържанието на файла (CNT) на записа тип-1 (поле 1.003).

4.1.3. Поле 2.003: Информация за системата (System Information — SYS)

Това поле е задължително и съдържа четири байта, с които се посочва на коя версия на INT-I съответства точно този запис тип-2.

Първите два байта посочват номера на основната версия, а вторите два — номера на подверсията. Например, в настоящия случай се работи по INT-I версия 4, редакция 22, което се изразява като „0422“.

4.1.4. Поле 2.007: Номер на случая (Case Number — CNO)

Този номер се задава от местната дактилоскопична служба за множеството следи, снети от едно местопрестъпление. Възприет е следният формат: CC/номер.

където „CC“ представлява кода на държавата по Интерпол, с дължина два буквено-цифрови символа, като *номерът* е съобразен с действащите на място указания и може да има дължина до 32 буквено-цифрови символа.

Това поле позволява на системата да идентифицира следи, които се свързват с определено местопрестъпление.

4.1.5. Поле 2.008: Номер на поредица (Sequence Number — SQN)

Посочва се всяка поредица от следи в рамките на същия случай. Дължината му е до четири цифрови символа. Поредицата представлява следа или поредица от следи, които са обединени за целите на документирането и/или търсенето. Съгласно тази дефиниция, на отделните единични следи също ще трябва да се даде номер на поредица.

Това поле може да се включи заедно с MID (поле 2.009), за да се идентифицира конкретна следа в поредицата.

4.1.6. Поле 2.009: Идентификатор на следа (Latent Identifier — MID)

Тук се посочва отделната следа в рамките на поредицата. Стойността представлява единична буква или две букви, като с „A“ се обозначава първата следа, с „B“ — втората и т.н. до „ZZ“. Това поле се използва аналогично на номера на поредицата следи, разгледан в описанието за SQN (поле 2.008).

4.1.7. Поле 2.010: Референтен номер на правонарушител (Criminal Reference Number — CRN)

Това е уникален референтен номер, който се задава от национален орган за лице, срещу което за пръв път е повдигнато обвинение за извършено престъпление. В рамките на една страна едно лице не може никога да има повече от един референтен номер на правонарушител (CRN), нито да го поделя с друго лице. За едно и също лице обаче е възможно да има референтни номера на правонарушител в различни държави, които се разпознават по кода на съответната държава.

За полето CRN е възприет следният формат: CC/номер

където „CC“ представлява кода на държавата по Интерпол, с дължина два буквено-цифрови символа, като *номерът* е съобразен с действащите национални указания на издаващия орган и може да има дължина до 32 буквено-цифрови символа.

За транзакциите по силата на Решение 2008/615/ПВР това поле ще се използва за националния референтен номер на правонарушителя, зададен от службата по произход, който е свързан с изображенията в записите тип-4 и тип-15.

4.1.8. Поле 2.012: Идентификационен номер — разни (Miscellaneous Identification Number — MN1)

В това поле се съдържа CRN (поле 2.010), изпратен чрез транзакция CPS или PMS без въвеждащия код за държавата.

4.1.9. Поле 2.013: Идентификационен номер — разни (Miscellaneous Identification Number — MN2)

В това поле се съдържа CNO (поле 2.007), изпратен чрез транзакция MPS или MMS без въвеждащия код за държавата.

4.1.10. Поле 2.014: Идентификационен номер — разни (Miscellaneous Identification Number — MN3)

В това поле се съдържа SQN (поле 2.008), изпратен чрез транзакция MPS или MMS.

4.1.11. Поле 2.015: Идентификационен номер — разни (Miscellaneous Identification Number — MN4)

В това поле се съдържа MID (поле 2.009), изпратен чрез транзакция MPS или MMS.

4.1.12. Поле 2.063: Допълнителна информация (Additional Information — INF)

В случай на транзакция SRE във връзка с искане PMS, в това поле се дава информация за пръста, за който се отнася евентуалното попадение (HIT). Полето се попълва във формат:

NN където „*NN*“ е кодът на позицията на пръста, определен в таблица 5, с дължина две цифри.

Във всички останали случаи това поле не е задължително. Състои се от най-много 32 буквено-цифрови символа и в него може да се даде допълнителна информация относно искането.

4.1.13. Поле 2.064: Списък на респондентите (Respondents List — RLS)

Това поле съдържа поне две подполета. В първото подполе се описва видът на извършеното търсене, като се използват трибуквени мнемонични съчетания, с които се определя типа транзакция в TOT (поле 1.004). Второто подполе съдържа само един символ. С „I“ се отбелязва наличие на попадение (HIT), а отсъствие на попадение (NOHIT) за търсения случай се отбелязва с „N“. В третото поле се съдържа идентификаторът на поредицата за кандидата за резултат и общият брой кандидати, разделени с наклонена черта. Ако кандидатите са повече от един, се отговаря с няколко съобщения. В случай на евентуално попадение (HIT) в четвъртото подполе се съдържа резултатът с дължина до шест символа.

Ако попадението (HIT) се потвърди, стойността на това подполе става „999999“.

Пример: „CPS{RS}I{RS}001/001{RS}999999{GS}“

Ако няма подаден резултат от отдалечената система AFIS, на съответното място се отбелязва нулев резултат.

4.1.14. Поле 2.074: Статус/поле за съобщение за грешка (Status/Error Message Field — ERM)

В това поле се съдържат съобщения за грешка в резултат на осъществена транзакция, които се изпращат на отправилата искането служба като част от транзакция за грешка.

Таблица 3: Съобщения за грешка

Numeric Code (1-3)	Meaning (5-128)
003	ERROR: UNAUTHORISED ACCESS
101	Mandatory field missing
102	Invalid record type
103	Undefined field
104	Exceed the maximum occurrence
105	Invalid number of subfields
106	Field length too short
107	Field length too long
108	Field is not a number as expected
109	Field number value too small
110	Field number value too big
111	Invalid character
112	Invalid date
115	Invalid item value
116	Invalid type of transaction
117	Invalid record data
201	ERROR: INVALID TCN
501	ERROR: INSUFFICIENT FINGERPRINT QUALITY
502	ERROR: MISSING FINGERPRINTS
503	ERROR: FINGERPRINT SEQUENCE CHECK FAILED
999	ERROR: ANY OTHER ERROR. FOR FURTHER DETAILS CALL DESTINATION AGENCY.

Съобщения за грешка с номер между 100 и 199:

Тези съобщения за грешка са свързани с валидирането на ANSI/NIST записите и се определят като:

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 2> FIELD <field_id 2> <dynamic text 2>...

където:

— error_code е код, зададен само за една определена причина (вж. таблица 3),

— field_id е ANSI/NIST номерът на сгрешеното поле (напр. 001, 2.001, ...) в следния формат <record_type>.-field_id>.sub_field_id>,

— dynamic text е по-подробното описание на грешката,

— LF означава „въвеждане на ред“ (Line Feed) и служи за разделяне на отделните грешки, когато има повече от една такава,

— за запис тип-1 се определя ICD „-1“.

Пример:

201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION

Това поле е задължително за транзакции за грешка.

4.1.15. Поле 2.320: Очакван брой кандидати (Expected Number of Candidates — ENC)

В това поле се съдържа максималният брой кандидати за верификация според отправилата искането служба. Стойността на ENC не може да надвишава стойностите, определени в таблица 11.

5. ***Логически запис тип-4: изображение с висока резолюция в сивата скала***

Следва да се отбележи, че записите тип-4 са по-скоро бинарни, отколкото ASCII по характер. Поради това на всяко поле в записа се задава определено място, от което се подразбира, че всички полета са задължителни.

Стандартът позволява в записа да се опишат както размерът на изображението, така и резолюцията. Изискването за логическите записи тип-4 е да съдържат данни на дактилоскопично изображение, което се предава с номинална наситеност 500—520 пиксела на инч. За по-новата техника, предпочитаната резолюция е 500 пиксела на инч или 19,68 пиксела на милиметър. В INT-I е посочена наситеност от 500 пиксела на инч, освен когато сходни системи могат да си общуват с друга резолюция в рамките на зададените предпочитани стойности от 500—520 пиксела на инч.

5.1. *Полета в логически запис тип-4:*

5.1.1. Поле 4.001: Дължина на логическия запис (Logical Record Length — LEN)

В това четирибайтово поле се дава дължината на настоящия запис тип-4 и се посочва общият брой на байтовете, като се включват всички байтове във всички полета на записа.

5.1.2. Поле 4.002: Символ за означение на изображението (Image Designation Character — IDC)

Това е еднобайтовият бинарен израз на номера на IDC, който е даден в заглавния файл.

5.1.3. Поле 4.003: Вид отпечатък (Impression Type — IMP)

Видът на отпечатъка е еднобайтово поле, което заема шестият байт на записа.

Таблица 4: Вид пръстов отпечатък

Code	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper
4	Latent impression captured directly
5	Latent tracing

Code	Description
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4. Поле 4.004: Позиция на пръста (Finger Position — FGP)

Това поле с фиксирана дължина от 6 байта заема позициите 7—12 на запис тип-4. В него се съдържат възможните пръстови позиции, като се започва от най-левия байт (7-ия байт на записа). Известната или най-вероятна пръстова позиция се взема от таблица 5. Възможно е да се посочат до пет допълнителни пръста, като пръстовите позиции се впишат в съответния порядък в оставащите пет байта, за което се използва същият формат. Ако се посочват по-малко от пет пръстови позиции, неизползваните байтове се запълват с бинарно 255. За реферирание на всички пръстови позиции се използва код „0“ със значение „неизвестно“.

Таблица 5: Код на пръстовите позиции и максимален размер

Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40,0	40,0
Right thumb	1	45,0	40,0
Right index finger	2	40,0	40,0
Right middle finger	3	40,0	40,0
Right ring finger	4	40,0	40,0
Right little finger	5	33,0	40,0
Left thumb	6	45,0	40,0
Left index finger	7	40,0	40,0
Left middle finger	8	40,0	40,0
Left ring finger	9	40,0	40,0
Left little finger	10	33,0	40,0
Plain right thumb	11	30,0	55,0
Plain left thumb	12	30,0	55,0
Plain right four fingers	13	70,0	65,0
Plain left four fingers	14	70,0	65,0

За следи, снети от местопрестъпление, се използват само кодовете от 0 до 10.

5.1.5. Поле 4.005: Резолюция на сканираното изображение (Image Scanning Resolution — ISR)

Това еднобайтово поле заема 13-ия байт на запис тип-4. Ако съдържа „0“, това означава, че изображението е направено с препоръчителната резолюция от 19,68 пиксела/mm (500 пиксела/инч). Ако съдържа „1“, това означава, че изображението е направено с алтернативната резолюция за сканиране, посочена в запис тип-1.

5.1.6. Поле 4.006: Дължина на хоризонталния ред (Horizontal Line Length — HLL)

Това поле се намира на мястото на байтове 14—15 в запис тип-4. В него се посочва броят на пикселите, които се съдържат във всеки ред на сканираното изображение. Най-съществен е първият байт.

5.1.7. Поле 4.007: Дължина на вертикалния ред (Vertical Line Length — VLL)

В 16-17 байт на това поле е записан броят на редовете на сканираното изображение. Най-съществен е първият байт.

5.1.8. Поле 4.008: Алгоритъм за компресиране в сивата скала (Greyscale Compression Algorithm — GCA)

В това еднобайтово поле се посочва алгоритъмът за компресиране в сивата скала, използван за кодиране на данните на изображението. За целите на прилагането, с бинарен код „1“ се посочва, че е използвана WSQ-компресия (допълнение 7).

5.1.9. Поле 4.009: Изображение

Това поле съдържа поредица от байтове, която представлява самото изображение. Структурата му очевидно зависи от използвания алгоритъм за компресиране.

6. ***Логически запис тип-9: запис на признаци (minutiae)***

Записите тип-9 съдържат ASCII-текст, описващ признаците (*minutiae*) и свързана кодирана информация от следи. При транзакция за търсене на следи няма ограничение за тези записи тип-9 в рамките на един файл, но всеки от тях следва да се отнася за различен изглед или следа.

6.1. *Извличане на признаци (minutiae)*

6.1.1. Идентификация на типа признак

С този стандарт се определят три идентификационни номера, които се използват за описване на типа признак. Изброени са в таблица 6. Край на папиларна линия се означава като тип 1. Бифуркация се означава като тип 2. Ако даден признак не може да се определи ясно като един от горепосочените типове, той се означава като „друг“ („other“) — тип „0“.

Таблица 6: Типове признаци

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Разположение и тип на признака

За да отговарят образците на раздел 5 от стандарта ANSI INCITS 378-2004, разположението (място и ъгъл на въртене) на отделния признак се описва по следния метод, който е усъвършенстван вариант на действащия стандарт INCITS 378-2004.

Позицията или местоположението на признака, който представлява край на папиларна линия, е точката на раздвояване на срединния скелет на междупапиларната бразда, разположена непосредствено пред края на папиларната линия. Ако трите отсечки на междупапиларната бразда се изтънят до скелет с широчина 1 пиксел, точката на пресичането им е местоположението на признака. Аналогично, местоположението на признака при бифуркация е точката на раздвояване на срединния скелет на папиларната линия. Ако всяка от трите отсечки на папиларната линия се изтъни до скелет с широчина 1 пиксел, точката на пресичане на трите отсечки е местоположението на признака.

След като всички краища на папиларни линии са преобразявани в бифуркации, всички признаци на дактилоскопичното изображение се представят под формата на бифуркации. Пикселовите координати X и Y на пресечната точка на трите отсечки на всеки признак могат да се форматират директно. Определянето на вектора на признака може да се извлече от всяка скелетна бифуркация. Трите отсечки на всяка скелетна бифуркация трябва да се разгледат и да се определи крайната точка на всяка отсечка. На фигура 6.1.2 са илюстрирани трите метода, които се използват за определяне на край на отсечка, което се прави на базата на сканираща резолюция 500 ppi.

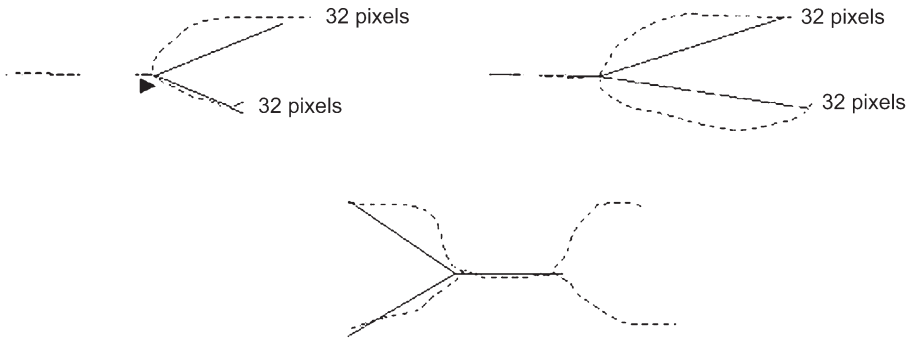
Краят се установява според това кое събитие се прояви първо. Броят на пикселите се определя на базата на образ, сканиран с резолюция 500 ppi. Подразбира се, че при друга резолюция ще се използва различен брой пиксели.

— Разстояние от .064” (32-ри пиксел)

— Краят на скелетната отсечка, която се появява в разстоянието между .02” и .064” (от 10-и до 32-ри пиксел); не се използват по-къси отсечки

— Втора бифуркация е открита на разстояние .064” (преди 32-рия пиксел)

Фигура 6.1.2



Ъгълът на признаците се определя, като се построят три виртуални лъча от точката на бифуркация до края на всяка отсечка. Ъглополовящата на най-малкия от трите ъгъла, образувани от лъчите, се използва за означаване на посоката на признака.

6.1.3. Координатна система

За изразяване на признаците на пръстов отпечатък се използва Декартова координатна система. Местоположението на признаците се представя от техните x и y координати. Началото на координатната система е горният ляв ъгъл на оригиналното изображение, като x нараства надясно, а y нараства надолу. И двете координати (x и y) на признаците се изразяват в пиксел единици, отстоящи от началото. Следва да се отбележи, че началната точка и мерните единици не съответстват на общоприетата система, използвана за дефинициите на тип-9 в ANSI/NIST-ITL 1-2000.

6.1.4. Ориентация на признаците

Ъглите се изразяват в стандартен математически формат, като нула градуса е вдясно и ъгълът расте обратно на часовниковата стрелка. Ъглите в записите са ориентирани по посоката на папиларната линия за край на папиларна линия и от центъра на междупапиларната бразда при бифуркация. Тази практика се разминава на 180 градуса със системата за определяне на ъглите, описана в дефинициите на тип-9 в ANSI/NIST-ITL 1-2000.

6.2. *Полета в логически запис тип-9, формат INCITS-378*

Всички полета от записите тип-9 се записват като ASCII текст. В този запис с тагови полета не се допускат бинарни полета.

6.2.1. Поле 9.001: Дължина на логическия запис (Logical record length — LEN)

В това задължително ASCII поле се съдържа дължината на логическия запис — посочва се общият брой на байтовете, като се включват всички байтове във всички полета на записа.

6.2.2. Поле 9.002: Символ за означение на изображението (Image designation character — IDC)

Това задължително двубайтово поле се използва за идентификация и описване на местоположението на данните за признаци. Записаният в това поле символ за IDC съответства на символа за IDC, който се намира в полето за съдържание на файла на записа тип-1.

6.2.3. Поле 9.003: Вид отпечатък (Impression type — IMP)

В това задължително еднобайтово поле се описва начинът, по който е получена информацията за дактилоскопичното изображение. ASCII стойността на самия код, която се взема от таблица 4, се вписва в това поле, за да се означи типът отпечатък.

6.2.4. Поле 9.004: Формат на признака (*Minutiae* format — FMT)

В това поле се съдържа „U“, за да се означи, че признаците са форматирани с M1-378. Въпреки че информацията може да е кодирана в съответствие със стандарта M1-378, всички полета за данни в записа тип-9 трябва да останат във формат ASCII-текст.

6.2.5. Поле 9.126: Информация CBEFF

В това поле се съдържат три информационни единици. Първата информационна единица има стойност „27“ (0x1B). Това е идентификацията на „притежателя“ на форма́та CBEFF, определена от Международната асоциация на биометричната индустрия (IBIA) за Техническия комитет INCITS M1. Тази единица се отделя с разделителен символ <US> от типа формат CBEFF, на който се задава стойност „513“ (0x0201), за да се означи, че в този запис се

съдържат само данни за местоположението и ъгловия вектор без информация за Extended Data Block. Тази единица се отделя с разделителен символ <US> от продуктовия идентификатор CBEFF (PID), с който се идентифицира „притежателят“ на кодиращото оборудване. Тази стойност се задава от фирмата производител. Стойността може да се вземе от уебсайта на IBIA (www.ibia.org), ако е публикувана там.

6.2.6. Поле 9.127: Идентификация на оборудването за „улавяне на образ“

В това поле има две информационни единици, разделени със символ <US>. Първата единица съдържа APPF, ако оборудването, използвано за добиване на първоначалния образ, има сертификат за съответствие с допълнение F (IAFIS Image Quality Specification, 29 януари, 1999 г.) по CJIS-RS-0010, спецификацията на Федералното бюро за разследване за изпращане на пръстови отпечатъци. Ако оборудването не отговаря на това изискване, се вписва стойност NONE. Втората информационна единица съдържа идентификацията на оборудването за „улавяне на образ“, която е продуктовият номер, зададен от фирмата-производител, за съответното оборудване. Стойност 0 показва, че идентификацията на оборудването за „улавяне на образ“ е неизвестна.

6.2.7. Поле 9.128: Дължина на хоризонталния ред (Horizontal line length — HLL)

В това задължително ASCII поле се съдържа броят на пикселите, които се съдържат в един хоризонтален ред на изпращаното изображение. Максималният размер на хоризонтален ред достига до 65 534 пиксела.

6.2.8. Поле 9.129: Дължина на вертикалния ред (Vertical line length — VLL)

В това задължително ASCII поле се задава броят на хоризонталните редове, които се съдържат в изпращаното изображение. Максималният размер на вертикален ред достига до 65 534 пиксела.

6.2.9. Поле 9.130: Мащабни единици (Scale units — SLC)

В това задължително ASCII-поле се посочват единиците, използвани за описание на честотата на дискретизация на изображението (плътност на пикселите). В това поле стойност 1 показва броя на пикселите на 1 инч, а 2 показва пикселите на 1 сантиметър. Стойност 0 в това поле показва, че не е даден мащаб. В този случай съотношението на страните на пикселите се определя като коефициент HPS/VPS.

6.2.10. Поле 9.131: Хоризонтален мащаб в пиксели (Horizontal pixel scale — HPS)

В това задължително ASCII поле се задава числото на плътността на пикселите по хоризонталата, при условие че в полето SLC има вписана стойност 1 или 2. В останалите случаи тя показва хоризонталния компонент на съотношението на страните на пикселите.

6.2.11. Поле 9.132: Вертикален мащаб в пиксели (Vertical pixel scale — VPS)

В това задължително ASCII поле се задава числото на плътността на пикселите по вертикалата, при условие че в полето SLC има вписана стойност 1 или 2. В останалите случаи тя показва вертикалния компонент на съотношението на страните на пикселите.

6.2.12. Поле 9.133: Пръстов изглед

В това задължително поле е даден номерът на изгледа на пръста, за който се отнасят данните в записа. Номерата на изгледите започват от 0 и нарастват с единица до 15.

6.2.13. Поле 9.134: Позиция на пръста (Finger position — FGP)

В това задължително поле се дава кодът, с който се означава позицията на пръста, от който е получена информацията в този запис тип-9. Позицията на пръста се посочва с код със стойности от 1 до 10, който се взема от таблица 5, а съответният код за позицията на длан се взема от таблица 10.

6.2.14. Поле 9.135: Качество на пръстовия отпечатък

Полето показва качеството на данните за признаците на пръстовия отпечатък като цяло и има стойност между 0 и 100. Това число е отражение на цялостното качество на записа за пръстовия отпечатък и представя качеството на оригиналното изображение, на извлечените признаци и всякакви допълнителни операции, които биха могли да повлияят на записа за признаците.

6.2.15. Поле 9.136: Брой признаци

В това задължително поле се съдържа броят на признаците, записани в този логически запис.

6.2.16. Поле 9.137: Данни за пръстовите признаци

В това поле има шест информационни единици, разделени със символ <US>. Състои се от няколко подполета, във всяко от които има подробни данни за един отделен признак. Общият брой на подполетата за признаци трябва да съответства на броя, посочен в поле 136. Първата информационна единица е индексният номер на признака, който започва от 1 и нараства с единица за всеки допълнителен признак на пръстовия отпечатък. Втората и третата информационна единица представляват „x“ и „y“ координатите на признаците, изразени в пиксели. Четвъртата информационна единица представлява ъгъла на признака, изразен в единици от по два градуса. Тази стойност е положително число между 0 и 179. Петата информационна единица изразява типа на признака. Със стойност 0 се представя тип „ДРУГО“ (OTHER), със стойност 1 се представя край на папиларна линия, а със стойност 2 — бифуркация на папиларната линия. Шестата информационна единица представлява качеството на съответния признак. Стойността ѝ варира между 1 за минималната стойност и 100 за максималната. Стойност 0 показва, че няма налична стойност за качеството. Всяко подполе се разделя от следващото с разделителен символ <RS>.

6.2.17. Поле 9.138: Информация за броя на папиларните линии

Това поле се състои от поредица подполета, във всяко от които има по три информационни единици. Първата информационна единица на първото подполе показва начина на получаване на броя на папиларните линии. Стойност 0 показва, че не могат да се правят никакви заключения относно начина на получаване на броя на папиларните линии, нито относно реда, в който са дадени в записа. Стойност 1 показва, че за всеки център на признак са получени данни за броя на папиларните линии до най-близките съседни признаци в четири квадранта, като броят на папиларните линии за всеки център на признак са изброени заедно. Стойност 2 показва, че за всеки център на признак са получени данни за броя на папиларните линии до най-близките съседни признаци в осем октанта, като броят на папиларните линии за всеки център на признак са изброени заедно. И двете останали информационни единици от първото подполе са със стойност 0. Информационните единици се разделят с разделителен символ <US>. В следващите подполета се съдържа индексният номер на центъра на признака като първа информационна единица, индексният номер на съседния признак като втора информационна единица и броят на пресечените папиларни линии като трета информационна единица. Подполетата се разделят с разделителен символ <RS>.

6.2.18. Поле 9.139: Информация за център на папиларен образ

Това поле се състои от по едно подполе за всеки наличен център на папиларен образ в оригиналното изображение. Всяко подполе съдържа три информационни единици. Първите две единици съдържат позиционните „x“ и „y“ координати, изразени в пиксели. Третата информационна единица съдържа ъгловата стойност на центъра на папиларния образ, изразена в единици от по 2 градуса. Стойността е положително число между 0 и 179. При повече центрове на папиларни образи, същите се разделят с разделителен символ <RS>.

6.2.19. Поле 9.140: Информация за делта

Това поле се състои от по едно подполе за всяка налична делта в оригиналното изображение. Всяко подполе съдържа три информационни единици. Първите две единици съдържат позиционните „x“ и „y“ координати, изразени в пиксели. Третата информационна единица съдържа ъгловата стойност на делтата, изразена в единици от по 2 градуса. Стойността е положително число между 0 и 179. При повече центрове на папиларни образи, същите се разделят с разделителен символ <RS>.

7. ***Запис тип-13 на изображение на следи с променлива резолюция***

Логическият запис тип-13 с тагови полета съдържа данни на изображение, получено от изображение на следи. Тези изображения са предназначени за изпращане на службите, които автоматично ще извлекат или ще осигурят интервенция на служители и обработка с цел получаване на желаната характеризираща информация от изображенията.

Под формата на тагови полета в записа се дава информация относно използваната резолюция на сканиране, размера на изображението и други параметри, необходими за обработката на изображението.

Таблица 7: Запис тип-13: изображение на следи с променлива резолюция

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13.003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
LCD	M	13.005	LATENT CAPTURE DATE	N	9	9	1	1	16

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
HLL	M	13.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	13.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13.011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	13.012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	13.013	FINGER POSITION	N	2	3	1	6	25
RSV		13.014 13.019	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
COM	O	13.020	COMMENT	A	2	128	0	1	135
RSV		13.021 13.199	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
UDF	O	13.200 13.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	13.999	IMAGE DATA	B	2	—	1	1	—

Легенда за вида символ: N = цифров; A = буквен; AN = буквено-цифров; B = бинарен

7.1. *Полета в логически запис тип-13:*

В следващите няколко параграфа са описани данните, които се съдържат във всяко от полетата в логически запис тип-13.

В логически запис тип-13 данните се въвеждат в номерирани полета. Изискването е първите две полета на записа да са подредени в установен ред, а полето, съдържащо данните на изображението е последното физическо поле в записа. В таблица 7 за всяко поле в запис тип-13 е посочен код за задължителност — задължително „M“ или незадължително „O“, номер на полето, наименование на полето, вид символ, размер на полето и колко пъти може да се използва. Използва се трицифрен номер на полето, като максималният брой на байтовете е даден в последната колонка. С увеличаване броя на цифрите в номера на полето се увеличава и максималният брой на байтовете. Двете стойности, които се вписват в „размер на полето за всяко използване“ се включват всички разделителни символи, използвани в полето. В „максималния брой байтове“ се включва номерът на полето, информацията и всички разделителни символи, в т.ч. и символът GS.

7.1.1. Поле 13.001: Дължина на логическия запис (Logical record length — LEN)

В това задължително ASCII поле е записано числото на общия брой байтове в целия логически запис тип-13. В поле 13.001 се посочва дължината на записа, като се включват всички символи във всички полета на записа плюс разделителите.

7.1.2. Поле 13.002: Символ за означение на изображението (Image designation character — IDC)

В това задължително ASCII поле се посочват данните за изображения на следи, които се съдържат в записа. Този IDC съответства на IDC, който се намира в полето за съдържание на файла (CNT) на записа тип-1.

7.1.3. Поле 13.003: Вид отпечатък (Impression type — IMP)

В това задължително еднобайтово или двубайтово ASCII поле се описва начинът, по който е получена информацията за изображението на следа. В това поле се вписва съответният код за следа, който се взема от таблица 4 (пръст) или от таблица 9 (длан).

7.1.4. Поле 13.004: Служба на произход/ORI (Source agency/ORI — SRC)

В това задължително ASCII поле се посочва идентификацията на службата или организацията, която първоначално е изготвила изображението на лице, което се съдържа в записа. В това поле обикновено се вписва идентификаторът на службата на произход (Originating Agency Identifier — ORI) за службата, която е изготвила изображението посредством „capture“ технология. Състои се от две информационни единици в следния формат: CC/служба.

Първата информационна единица съдържа кода на държавата по Интерпол — два буквено-цифрови символа. Втората единица, *службата*, представлява свободен текст за идентификация на службата — не повече от 32 буквено-цифрови символа.

7.1.5. Поле 13.005: Дата на изготвяне на изображението на следи (Latent capture date — LCD)

В това задължително ASCII поле се посочва датата, на която е изготвено изображението на следи, които се съдържат в записа. Датата се изписва с осем цифри във формат CCYYMMDD. Символите за CCYY представляват годината, в която е изготвено изображението; символите за MM представляват стойностите за десетицата и единицата на месеца; а символите за DD представляват стойностите за десетицата и единицата на деня от месеца; например 20000229 означава 29 февруари 2000 г. Пълната дата трябва да е действителна дата.

7.1.6. Поле 13.006: Дължина на хоризонталния ред (Horizontal line length — HLL)

В това задължително ASCII поле се задава броят на пикселите, които се съдържат в един хоризонтален ред на изпращаното изображение.

7.1.7. Поле 13.007: Дължина на вертикалната линия (Vertical line length — VLL)

В това задължително ASCII поле се задава броят на хоризонталните редове, които се съдържат в изпращаното изображение.

7.1.8. Поле 13.008: Мащабни единици (Scale units — SLC)

В задължително ASCII-поле се посочват единиците, използвани за описание на честотата на дискретизация на изображението (плътност на пикселите). В това поле стойност 1 показва броя на пикселите на 1 инч, а 2 показва пикселите на 1 сантиметър. Стойност 0 в това поле показва, че не е даден мащаб. В този случай съотношението на страните на пикселите се определя като коефициент HPS/VPS.

7.1.9. Поле 13.009: Хоризонтален мащаб в пиксели (Horizontal pixel scale — HPS)

В това задължително ASCII поле се задава числото на плътността на пикселите по хоризонталата, при условие че в полето SLC има вписана стойност 1 или 2. В останалите случаи тя показва хоризонталния компонент на съотношението на страните на пикселите.

7.1.10. Поле 13.010: Вертикален мащаб в пиксели (Vertical pixel scale — VPS)

В това задължително ASCII поле се задава числото на плътността на пикселите по вертикалата, при условие че в полето SLC има вписана стойност 1 или 2. В останалите случаи тя показва вертикалния компонент на съотношението на страните на пикселите.

7.1.11. Поле 13.011: Алгоритъм за компресиране (Compression algorithm — CGA)

В това задължително ASCII поле се посочва алгоритъмът, използван за компресиране на изображения в сивата скала. Вижте в допълнение 7 кодовете за компресия.

7.1.12. Поле 13.012: Битове на пиксел (Bits per pixel — BPX)

В това задължително ASCII поле се посочва броят на битовете, използвани за представяне на един пиксел. В това поле се вписва 8 за нормалните стойности на сивата скала от 0 до 255. Когато в това поле е въведена стойност, по-голяма от 8, това означава по-висока степен на пикселиране в сивата скала.

7.1.13. Поле 13.013: Позиция на пръста/дланта (Finger/palm position — FGP)

В това задължително тагово поле се вписва позицията или позициите на пръста или дланта, които е възможно да съвпаднат с изображението на следата. Десетичното кодово число, което съответства на известната или най-вероятна пръстова позиция, се взема от таблица 5, а за най-вероятна позиция на дланта — от таблица 10, и се вписва като едносимволно или двусимволно ASCII подполе. Допълнителни позиции за пръст и/или длан могат да се посочат като се впишат алтернативните позиционни кодове под формата на подполета, отделени с разделителен символ RS. Кодът 0 — за „неизвестен пръст“, се използва за рефериране на всяка пръстова позиция от едно до десет. Кодът 20 — за „неизвестна длан“, се използва за рефериране на всяка вписана позиция на длан.

7.1.14. Полета 13.014-019: Резервирано за по-нататъшно дефиниране (Reserved for future definition — RSV)

Тези полета са резервирани за включване в по-нататъшни редакции на настоящия стандарт. Никое от тези полета не се използва на този етап на редактиране. Ако някое от тези полета е запълнено, то не се взема под внимание.

7.1.15. Поле 13.020: Бележки (Comment — COM)

Това незадължително поле може да се използва за вписване на бележки или на друга информация с ASCII-текст към данните за изображение на следи.

7.1.16. Полета 13.021-199: Резервирано за по-нататъшно дефиниране (Reserved for future definition — RSV)

Тези полета са резервирани за включване в по-нататъшни редакции на настоящия стандарт. Никое от тези полета не се използва на този етап на редактиране. Ако някое от тези полета е запълнено, то не се взема под внимание.

7.1.17. Полета 13.200-998: Полета, дефинирани от потребителя (User-defined fields — UDF)

Тези полета могат да се дефинират от потребителя и се използват за бъдещи изисквания. Размерът и съдържанието им се определят от потребителя и са съгласувани със службата получател. Когато са попълнени, в тях се съдържа информация под формата на ASCII текст.

7.1.18. Поле 13.999: Данни на изображението (Image data — DAT)

В това поле се намират всички данни на изображението на следа, направено посредством „capture“ технология. Полето винаги има стойност 999 и е последното физически разположено поле в записа. Например: след „13.999:“ има бинарно представени данни на изображение.

Всеки пиксел от некомпресирани данни в сивата скала обикновено се изразяват количествено в осем бита (256 нива на сивото), които се съдържат в един байт. Ако в BPX поле 13.012 е вписана стойност по-голяма или по-малка от 8, броят на байтовете, в които се съдържа един пиксел, е различен. Ако се използва компресия, пиксел-данните трябва да се компресират по начина, определен в полето GCA начин.

7.2. *Край на запис тип-13: изображение на следи с променлива резолюция*

За по-голяма прегледност, непосредствено след последния байт данни на поле 13.999 се поставя разделител FS, за да се раздели този от следващия логически запис. Този разделител трябва да се включи в полето за дължината на запис тип-13.

8. ***Запис тип-15: изображение на отпечатък от длан с променлива резолюция***

Логически запис тип-15 с тагови полета съдържа и се използва за обмен на данни за изображение на отпечатък от длан, като в него има полета за фиксирана информация и за определена от потребителя информация, свързана с цифровизираното изображение. Под формата на тагови полета в записа се дава информация относно използваната резолюция на сканиране, размера на изображението и други параметри или бележки, необходими за обработката на изображението. Изпращаните на други служби изображения на длан се обработват от службите-получатели за извличане на желаната характеризираща информация, необходима за целите на сравняването.

Данните на изображението се получават пряко от субект, който използва уред за сканиране на живо или карта, на която е снет отпечатък на длан, или други носители, на които има отпечатък на длан.

Какъвто и да е методът за добиване на изображението на отпечатъка на длан, той трябва да има възможност за снемане на определен набор от изображения за всяка ръка. Този набор включва хипотенарната част на дланта, под формата на единично сканирано изображение, и пълната зона на изпънатата цяла длан от китката до върха на пръстите под формата на едно или две сканирани изображения. Ако са използвани две изображения за представяне на цялата длан, долното изображение показва дланта от китката до върха на междупръстието (ставата на третия пръст) и включва тенарната и хипотенарната област на дланта. Горното изображение обхваща зоната от долния край на междупръстието до върха на пръстите. По този начин се осигуряват достатъчно голяма зона на припокриване на двете изображения, и двете от които включват междупръстието на дланта. Чрез сравняване на папиларните линии и детайлите, които се съдържат в тази обща част, провеждащият изследването може да твърди с увереност, че двете изображения са на една и съща длан.

Тъй като транзакцията за отпечатък на длан може да се използва за различни цели, тя може да съдържа изображения на една или повече уникални зони на дланта или цялата ръка. Пълният набор от отпечатъци на дланта на едно лице обикновено включва хипотенарната част на дланта и изображение(я) на цялата длан от всяка ръка. Тъй като логическият запис с тагови полета, който се използва за изображение, може да съдържа само едно бинарно поле, за всяка хипотенарна част на длан ще е необходим отделен запис тип-15, както и едни или два записа тип-15 за всяка цяла длан. Поради това ще са необходими 4 — 6 записа тип-15 за представяне на отпечатъците от длан на даден субект в една нормална транзакция за отпечатъци на длан.

8.1. *Полета в логически запис тип-15:*

В следващите няколко абзаца са описани данните, които се съдържат във всяко от полетата в логически запис тип-15.

В логически запис тип-15 данните се въвеждат в номерирани полета. Изискването е първите две полета на записа да са подредени в установен ред, а полето с данните на изображението е последното физическо поле в записа. В таблица 8 за всяко поле в запис тип-15 е посочен код за задължителност — задължително „M“ или незадължително „O“, номер на полето, наименование на полето, вид символ, размер на полето и колко пъти може да се използва. Използва се трицифрен номер на полето, като максималният брой на байтовете е даден в последната колонка. С увеличаване броя на цифрите в номера на полето се увеличава и максималният брой на байтовете. Двете стойности, които се вписват в „размер на полето за всяко използване“. В „максималния брой байтове“ се включва номерът на полето, информацията и всички разделителни символи, в т.ч. и символът GS.

8.1.1. Поле 15.001: Дължина на логическия запис (Logical record length — LEN)

В това задължително ASCII поле е записано числото на общия брой байтове в целия логически запис тип-15. В поле 15.001 се посочва дължината на записа, като се включват всички символи във всички полета на записа плюс разделителите.

8.1.2. Поле 15.002: Символ за означение на изображението (Image designation character — IDC)

Това задължително ASCII поле се използва за идентифициране на изображението на отпечатък от длан, което се съдържа в записа. Този IDC съответства на IDC, който се намира в полето за съдържание на файла (CNT) на записа тип-1.

8.1.3. Поле 15.003: Вид отпечатък (Impression type — IMP)

В това задължително еднобайтово ASCII поле се посочва начинът, по който е получена информацията за изображението на отпечатъка на длан. В това поле се вписва съответният код, който се взема от таблица 9.

8.1.4. Поле 15.004: Служба на произход/ORI (Source agency/ORI — SRC)

В това задължително ASCII поле се вписва идентификацията на службата или организацията, която първоначално е изготвила изображението на лице, което се съдържа в записа. В това поле обикновено се вписва идентификаторът на службата на произход (ORI) за съответната служба, която е изготвила изображението посредством „capture“ технология. Състои се от две информационни единици в следния формат: CC/служба.

Първата информационна единица съдържа кода на държавата по Интерпол — два буквено-цифрови символа. Втората единица, *службата*, представлява свободен текст за идентификация на службата — не повече от 32 буквено-цифрови символа.

8.1.5. Поле 15.005: Дата на изготвяне на изображението на отпечатък от длан посредством „capture“ технология (Palmprint capture date — PCD)

В това задължително ASCII поле се вписва датата, на която е изготвено изображението на отпечатък от длан посредством capture-технология. Датата се изписва с осем цифри във формат CCYYMMDD. Символите за CCYY представляват годината, в която е изготвено изображението; символите за MM представляват стойностите за десетицата и единицата на месеца; а символите за DD представляват стойностите за десетицата и единиците на деня от месеца; например, вписаната стойност 20000229 означава 29 февруари 2000 г. Пълната дата трябва да е действително съществуваща дата.

8.1.6. Поле 15.006: Дължина на хоризонталния ред (Horizontal line length — HLL)

В това задължително ASCII поле се задава броят на пикселите, които се съдържат в един хоризонтален ред на изпращаното изображение.

8.1.7. Поле 15.007: Дължина на вертикалната линия (Vertical line length -VLL)

В това задължително ASCII поле се задава броят на хоризонталните редове, които се съдържат в изпращаното изображение.

8.1.8. Поле 15.008: Мащабни единици (Scale units — SLC)

В задължително ASCII-поле се посочват единиците, използвани за описание на честотата на дискретизация на изображението (плътност на пикселите). В това поле стойност 1 показва броя на пикселите на 1 инч, а 2 показва пикселите на 1 сантиметър. Стойност 0 в това поле показва, че не е даден мащаб. В този случай съотношението на страните на пикселите се определя като коефициент HPS/VPS.

8.1.9. Поле 15.009: Хоризонтален мащаб в пиксели (HPS)

В това задължително ASCII поле се задава числото на наситеност с пиксели по хоризонталата, при условие че в полето SLC има вписана стойност 1 или 2. В останалите случаи тя показва хоризонталния компонент на съотношението на страните на пикселите.

8.1.10. Поле 15.010: Вертикален мащаб в пиксели (Horizontal pixel scale — VPS)

В това задължително ASCII поле се задава числото на наситеност с пиксели по вертикалата, при условие че в полето SLC има вписана стойност 1 или 2. В останалите случаи тя показва вертикалния компонент на съотношението на страните на пикселите.

Таблица 8: Схема на запис тип-15 на изображение на отпечатък от длан с променлива резолюция

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
COM	O	15.020	COMMENT	AN	2	128	0	1	128
RSV		15.021 15.199	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
UDF	O	15.200 15.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	15.999	IMAGE DATA	B	2	—	1	1	—

Таблица 9: Вид изображение на длан

Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11. Поле 15.011: Алгоритъм за компресиране (Compression algorithm — CGA)

В това задължително ASCII поле се посочва алгоритъмът, използван за компресиране на изображения в сивата скала. Ако в полето е вписано „NONE“, това показва, че данните в този запис не са компресирани. За изображенията, които следва да се компресират, в това поле се вписва предпочитаният метод на компресиране за изображения с десет пръстови отпечатъка. Валидните кодове за компресията са дефинирани в допълнение 7.

8.1.12. Поле 15.012: Битове на пиксел (Bits per pixel — BPX)

В това задължително ASCII поле се посочва броят на битовете, използвани за представяне на един пиксел. В това поле се вписва 8 за нормалните стойности на сивата скала от 0 до 255. Когато в това поле е въведена стойност, по-голяма или по-малка от 8, това означава съответно по-висока или по-ниска степен на пикселиране в сивата скала.

Таблица 10: Кодове, зони и размери на длан

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28 387	139,7	203,2
Right Full Palm	21	28 387	139,7	203,2
Right Writer s Palm	22	5 645	44,5	127,0
Left Full Palm	23	28 387	139,7	203,2
Left Writer s Palm	24	5 645	44,5	127,0
Right Lower Palm	25	19 516	139,7	139,7
Right Upper Palm	26	19 516	139,7	139,7
Left Lower Palm	27	19 516	139,7	139,7
Left Upper Palm	28	19 516	139,7	139,7
Right Other	29	28 387	139,7	203,2
Left Other	30	28 387	139,7	203,2

8.1.13. Поле 15.013: Позиция на отпечатъка на длан (Palmprint position — PLP)

В това задължително тагово поле се описва позицията на отпечатъка от длан, съответстваща на изображението на отпечатъка от длан. Десетичният код, съответстващ на известната или най-вероятна позиция на отпечатъка от длан, се взема от таблица 10 и се вписва като двусимволно ASCII подполе. В таблица 10 също така са изброени максималните стойности за площта и размерите на изображението за всяка от възможните позиции на отпечатъка от длан.

8.1.14. Полета 15.014-019: Резервирано за по-нататъшно дефиниране (Reserved for future definition — RSV)

Тези полета са резервирани за включване в по-нататъшни редакции на настоящия стандарт. Никое от тези полета не се използва на този етап на редактиране. Ако някое от тези полета е запълнено, то не се взема под внимание.

8.1.15. Поле 15.020: Бележки (Comment — COM)

Това незадължително поле може да се използва за вписване на бележки или на друга информация с ASCII-текст към данните за изображение на отпечатък от длан.

8.1.16. Полета 15.021-199: Резервирано за по-нататъшно дефиниране (Reserved for future definition — RSV)

Тези полета са резервирани за включване в по-нататъшни редакции на настоящия стандарт. Никое от тези полета не се използва на този етап на редактиране. Ако някое от тези полета е запълнено, то не се взема под внимание.

8.1.17. Полета 15.200-998: Полета, дефинирани от потребителя (User-defined fields — UDF)

Тези полета могат да се дефинират от потребителя и се използват за бъдещи изисквания. Размерът и съдържанието им се определят от потребителя и са съгласувани със службата-получател. Когато са попълнени, в тях се съдържа информация под формата на ASCII-текст.

8.1.18. Поле 15.999: Данни на изображението (Image data — DAT)

В това поле се намират всички данни на изображението на отпечатък от длан, направено посредством capture-технология. Полето винаги има стойност 999 и е последното физически разположено поле в записа. Например: след „15.999:“ има бинарно представени данни на изображение. Всеки пиксел от некомпресирани данни в сивата скала обикновено се изразяват количествено в осем бита (256 нива на сивото), които се съдържат в един байт. Ако в BPX поле 15.012 е вписана стойност по-голяма или по-малка от 8, броят на байтовете, в които се съдържа един пиксел, е различен. Ако се използва компресия, пиксел-данните трябва да се компресират по начина, определен в полето CGA начин.

8.2. *Край на запис тип-15 на изображение на отпечатък на длан с променлива резолюция*

За по-голяма прегледност, непосредствено след последния байт данни на поле 15.999 се поставя разделител FS, за да се раздели този от следващия логически запис. Този разделител трябва да се включи в полето за дължината на запис тип-15.

8.3. *Допълнителни записи тип-15: изображение на длан с променлива резолюция*

Във файла могат да се включат допълнителни записи тип-15. За всяко допълнително изображение на отпечатък от длан е необходим цял логически запис тип-15 заедно със съответния FS разделител.

Таблица 11: Максимален допустим брой на кандидатите, които се подават за сверяване в едно съобщение

Type of AFIS Search	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Maximum Number of Candidates	1	10	5	5	5	5	5

Видове търсения:

TP/TP: десет пръстови отпечатъка спрямо десет пръстови отпечатъка (ten-print against tenprint)

LT/TP: отпечатък от пръстови следи спрямо десет пръстови отпечатъка (fingerprint latent against ten-print)

LP/PP: следи от отпечатък от длан спрямо отпечатък от длан (palmprint latent against palmprint)

TP/UL: десет пръстови отпечатъка спрямо отпечатък от неопределена пръстова следа (ten-print against unsolved fingerprint latent)

LT/UL: отпечатък от пръстова следа спрямо отпечатък от неопределена пръстова следа (fingerprint latent against unsolved fingerprint latent)

PP/ULP: отпечатък от длан спрямо неопределен отпечатък от длан (palmprint against unsolved palmprint latent)

LP/ULP: следа от отпечатък от длан спрямо неопределен отпечатък от длан (palmprint latent against unsolved palmprint latent)

9. ***Допълнения към глава 2 (обмен на дактилоскопични данни)***

9.1. *Допълнение 1 ASCII разделителни кодове*

ASCII	Position ([1])	Description
LF	1/10	Separates error codes in field 2.074
FS	1/12	Separates logical records of a file
GS	1/13	Separates fields of a logical record
RS	1/14	Separates the subfields of a record field
US	1/15	Separates individual information items of the field or subfield

([1]) Това е позицията съгласно определеното в ASCII-стандарта.

9.2. *Допълнение 2 Изчисляване на буквено-цифровия контролен символ*

За TCN и TCR (полета 1.09 и 1.10):

Числото, съответстващо на контролния символ, се генерира по следната формула:

(YY * 10^8 + SSSSSSSS) Modulo 23

където YY и SSSSSSSS са числовите стойности, съответстващи на последните две цифри от годината и на серийния номер.

Контролният символ се генерира по дадената по-долу справочна таблица.

За CRO (поле 2.010)

Числото, съответстващо на контролния символ, се генерира по следната формула:

(YY * 10^6 + NNNNNN) Modulo 23

където YY и NNNNNN са числовите стойности, съответстващи на последните две цифри от годината и на серийния номер.

Контролният символ се генерира по дадената по-долу справочна таблица.

Справочна таблица за контролните символи

1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

9.3. *Допълнение 3 Символни кодове*

7-битов ANSI код за информационен обмен

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	”	#	$	%	&	’
40	(	)	*	+	,	—	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

9.4. *Допълнение 4 Кратко описание на транзакция*

Запис тип-1 (задължителен)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

В колонката за задължителност:

O = незадължително; M = задължително; C = в зависимост от това дали транзакцията представлява отговор, изпратен до службата на произход

Запис тип-2 (задължителен)

Identifier	Field Number	Field Name	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

В колонката за задължителност:

O.= незадължително; M = задължително; C = в зависимост от това дали има налични данни

* = ако предаването на данните е в съответствие с националното законодателство (не попада в обхвата на Решение 2008/615/ПВР)

9.5. *Допълнение 5 Дефиниции на запис тип-1:*

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{US}15{RS}2{US}00{RS}4 {US}01{RS}4{US}02{RS}4{US}03 {RS}4{US}04{RS}4{US}05{RS}4 {US}06{RS}4{US}07{RS}4{US}08 {RS}4{US}09{RS}4{US}10{RS}4 {US}11{RS}4{US}12{RS}4{US}13 {RS}4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{GS}
DAT	M	1.005	Date	N	1.005:20050101{GS}
PRY	M	1.006	Priority	N	1.006:4{GS}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1.013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

В колонката за задължителност: O = незадължително, M = задължително, C = под условие

В колонката за вид символ: A = буквен, N = числов, B = бинарен

1* допустими символи за наименованието на службата [„0..9“, „A..Z“, „a..z“, „_“, „.“, „ “, „—“]

9.6. *Допълнение 6 Запис тип-2: дефиниции*

Таблица A.6.1: Транзакции CPS и PMS

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	M	2.010	Criminal Reference Number	AN	2.010:DE/E999999999{GS}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Таблица A.6.2: Транзакция SRE

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	C	2.010	Criminal Reference Number	AN	2.010:NL/2222222222{GS}
MN1	C	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
RLS	M	2.064	Respondents List	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

Таблица A.6.3: Транзакция ERR

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
MN1	M	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {GS}

Таблица A.6.4: Транзакции MPS и MMS

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CNO	M	2.007	Case Number	AN	2.007:E999999999{GS}
SQN	C	2.008	Sequence Number	N	2.008:0001{GS}
MID	C	2.009	Latent Identifier	A	2.009:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123 {GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

В колонката за задължителност: O = незадължително, M = задължително, C = под условие

В колонката за вид символ: A = буквен, N = числов, B = бинарен

1* допустимите символи са [„0..9“, „A..Z“, „a..z“, „_“, „.“, „ “, „—“]

9.7. *Допълнение 7 Кодове за компресия в сивата скала*

Кодове за компресия

Compression	Value	Remarks
Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated December 19, 1997	WSQ	Algorithm to be used for the compression of grayscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions > 500 dpi.
JPEG 2000 [ISO 15444/ITU T.800]	J2K	To be used for lossy and losslessly compression of grayscale images in Type-13 to Type-15 records. Strongly recommended for resolutions > 500 dpi.

9.8. *Допълнение 8 Спецификация на съобщенията*

За подобряване на вътрешните работни процеси, в полето „Предмет“ на транзакциите, осъществявани по линия на Прюм, трябва да се попълнят кодът (CC) на държавата-членка, която изпраща съобщението, и типът на транзакцията (TOT поле 1.004)

Формат: CC/тип транзакция

Пример: „DE/CPS“

Съобщението може да бъде без съдържание.

ГЛАВА 3: **Обмен на данни за регистрацията на превозни средства**

1. ***Общ набор от данни за автоматизирано търсене на данни за регистрацията на превозни средства***

1.1. *Определения*

Определенията за задължителните елементи и незадължителните елементи на данните, посочени в член 16, параграф 4, са следните:

Задължително (M):

Този елемент трябва да бъде съобщен, когато има налична информация в националния регистър на държавата-членка. Следователно информацията се обменя задължително, когато е налична.

Незадължително (O):

Този елемент може да бъде съобщен, когато има налична информация в националния регистър на държавата-членка. Следователно не е задължително да се обменя информация, дори когато тя е налична.

Всеки елемент от набора данни се обозначава с (Y), когато този елемент се определя като особено важен във връзка с Решение 2008/615/ПВР.

1.2. *Търсене на превозно средство/собственик/ползвател*

1.2.1. Повод за търсене

Съществуват два различни начина за търсене на информацията, които са определени по-долу:

— по номер на шасито (VIN), референтна дата и час (незадължително);

— по табела с регистрационния номер, по номер на шасито (VIN) (незадължително), референтна дата и час (незадължително).

Посредством тези критерии за търсене се получава информация, свързана с едно, а понякога и повече превозни средства. Ако се получи информация само за едно превозно средство, всички единици информация се поместват в един отговор. Ако са намерени повече превозни средства, държавата-членка, към която е отправено искането, може да определи кои информационни единици да изпрати в отговора — всички единици или само единиците, с които да се усъвършенства търсенето (напр. поради съображения, свързани с неприкосновеността на личния живот, или съображения за качество на работата).

Информационните единици, необходими за усъвършенстване на търсенето, са дадени в точка 1.2.2.1. В точка 1.2.2.2 е описана изчерпателно цялата информация.

Когато се прави търсене по номер на шаси, референтна дата и час, то може да се направи в една от участващите държави-членки или във всичките.

Когато се прави търсене по номер на свидетелство за управление, референтна дата и час, то трябва да се направи в една конкретна държава-членка.

Обикновено за търсене се използват датата и часът към момента, но е възможно да се извърши търсене с референтна дата и час в миналото. Когато се извършва търсене по референтна дата и час в миналото, а историческа информация не е налична в регистъра на съответната държава-членка, понеже такава регистрирана информация отсъства, информацията може да се изпрати, като се посочи, че тази информация е информация към момента.

1.2.2. Набор от данни

1.2.2.1. Данни, които се дават в отговора с цел прецизиране на търсенето

Item	M/O [1]	Remarks	Prüm Y/N [2]
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1 [3]) e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y

Item	M/O (1)	Remarks	Prüm Y/N (2)
EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y

(1) M = задължително, когато са налице данни в националния регистър, O = незадължително.
(2) Всички атрибути, специално придадени от държавите-членки, се обозначават с Y.
(3) Хармонизирани съкращения за документите, вж. Директива 1999/37/ЕО на Съвета от 29 април 1999 г.

1.2.2.2. Пълен набор от данни

Item	M/O (1)	Remarks	Prüm Y/N
Data relating to holders of the vehicle		(C.1 (2)) The data refer to the holder of the specific registration certificate.	
Registration holders' (company) name	M	(C.1.1) separate fields will be used for surname, infixes, titles etc., and the name in printable format will be communicated	Y
First name	M	(C.1.2) separate fields for first name(s) and initials will be used, and the name in printable format will be communicated	Y
Address	M	(C.1.3) separate fields will be used for Street, House number and Annex, Zip code, Place of residence, Country of residence etc., and the Address in printable format will be communicated	Y
Gender	M	Male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle.	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: — is the vehicle owner — is not the vehicle owner — is not identified by the registration certificate as being the vehicle owner	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y

Item	M/O [1]	Remarks	Prüm Y/N
Address	M	(C.2.3)	Y
Gender	M	male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date ownership	O	Start date of the ownership of the car.	N
End date ownership	O	End data of the ownership of the car.	N
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1) e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
Nature of the vehicle/EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y
Date of first registration	M	(B) date of first registration of the vehicle somewhere in the world	Y
Start date (actual) registration	M	(I) Date of the registration to which the specific certificate of the vehicle refers	Y
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H).	Y
Status	M	scrapped, stolen, exported etc.	Y
Start date status	M		Y
End date status	O		N
kW	O	(P.2)	Y
Capacity	O	(P.1)	Y
Type of licence number	O	regular, transito etc.	Y
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document	Y
Vehicle document id 2 [3]	O	A second document ID as printed on the vehicle document.	Y
Data relating to insurances			
Insurance company name	O		Y
Begin date insurance	O		Y
End date insurance	O		Y
Address	O		Y
Insurance number	O		Y

Item	M/O (1)	Remarks	Prüm Y/N
ID Number	O	An identifier that uniquely identifies the company.	N
Type of ID Number	O	The type of ID Number (e.g. number of the Chamber of Commerce)	N

(1) M = задължително, когато са налице данни в националния регистър, O = незадължително.
(2) Хармонизирани съкращения за документите, вж. Директива 1999/37/ЕО на Съвета от 29 април 1999 г.
(3) В Люксембург се използват два различни вида документи за регистрация на превозно средство.

2. ***Сигурност на данните***

2.1. *Обзорен преглед*

Софтуерното приложение EUCARIS се използва за защитена комуникация с другите държави-членки и за съобщения, подавани в XML-формат обратно към „наследените“ системи на държавите-членки. Държавите-членки обменят съобщения, като ги изпращат директно на получателя. Центърът за електронни данни на държавата-членка е свързан с мрежата TESTA на ЕС.

По мрежата се изпращат криптирани съобщения в XML-формат. За криптиране на съобщенията се използва методът SSL. Съобщенията, които се връщат обратно, са в обикновен текстови XML-формат, тъй като връзката между приложението и т.нар. „back-end“ става в защитена среда.

Осигурено е клиентско програмно приложение, което се използва в държавата-членка за търсене в собствения ѝ регистър или в регистрите на другите държави-членки. Клиентите се идентифицират посредством потребителско име за идентификация/парола или клиентски сертификат. Връзката с потребителя може да е криптирана, но това е задължение на всяка отделна държава-членка.

2.2. *Характеристики на сигурността, свързани с обмена на съобщения*

Сигурността е проектирана на основата на съчетание от HTTPS и XML-подпис. При този вариант се използва XML-подпис за подписване на всички съобщения, които се изпращат до сървъра, като чрез проверка на подписа се удостоверява кой е подателят на съобщението. Едностранен SSL (само сертификат на сървъра) се използва за защита на поверителността и целостта на съобщението по време на изпращане и се осигурява защита от атаки с цел изтриване/„прослушване“ или вмъкване. Вместо първоначално предвидената разработка на софтуер за внедряване на двустранен SSL, беше внедрен XML-подпис. Използването на XML-подпис се доближава повече до пътната карта на уебуслугите отколкото двустранният SSL и следователно е по-стратегическо решение.

XML-подписът може да се внедри по няколко начина, но избраният подход е да се използва XML-подпис като част от сигурността на услугите в глобалната мрежа (WSS). В WSS се уточнява как да се използва XML-подписът. Тъй като WSS е разработен на основата на стандарта SOAP, логично е да спазваме възможно най-точно стандарта SOAP.

2.3. *Характеристики на сигурността, несвързани с обмена на съобщения*

2.3.1. Автентикация на потребителите

Автентикацията на потребителите на уебприложението Eucaris се осъществява посредством потребителско име и парола. Тъй като се използва стандартната автентикация на Windows, държавите-членки могат при необходимост да увеличат степента на автентикация на потребителите, като използват клиентски сертификати.

2.3.2. Функции на потребителя

Софтуерното приложение на Eucaris поддържа различни потребителски функции. За всяка категория услуги се получава отделно разрешение — напр. потребители (с изключителни права) на функционалността „Договор за Eucaris“ нямат право да използват функционалността „Прюм“. Услугите по администрирането са отделени от обичайните функции на крайния потребител.

2.3.3. Регистриране и проследяване на обмен на съобщения

Регистрирането на всички видове съобщения е улеснено от софтуерното приложение Eucaris. Посредством една от функциите за администриране националният администратор може да установи кои съобщения са регистрирани: искания от крайни потребители, входящи искания от други държави-членки, информация, предоставяна от национални регистри и т.н.

Приложението може да се конфигурира при това регистриране да използва вътрешна база данни или външна база данни (Oracle). Ясно е, че решението за това какви съобщения да се регистрират зависи от съоръженията за тази цел на други места — в „наследените“ системи, и от това с какви клиентски приложения има връзка.

В заглавната част на всяко съобщение се съдържа информация за отправилата искането държава-членка, съответната организация в държавата-членка и крайния потребител. Посочва се и поводът за отправяне на искането.

Посредством комбинираното регистриране в двете държави — отправилата искането и отговарящата — е възможно да се проследи напълно всеки обмен на съобщения (напр. по искане на замесено лице).

Регистрирането се потвърждава чрез уебклиента на Eucaris (меню Administration, Logging configuration). Функционалността за регистрирането се изпълнява от централната система. Когато е активирана функцията за регистриране, цялото съобщение (заглавна и съдържателна част) се съхранява в един регистърен запис. Възможно е да се зададе ниво на регистриране за определена услуга и за вид съобщения.

Нива на регистриране

Възможни са следните нива на регистриране:

Private — регистриране на съобщение: Регистрирането НЕ е достъпно за регистърната услуга за извличане, но е достъпно само на национално равнище, за одитиране и решаване на проблеми.

None — съобщението не се регистрира.

Видове съобщения

В информационния обмен между държавите-членки се включват различни видове съобщения, които са представени схематично по-долу.

Възможните видове съобщения (в показаната на фигурата централна система Eucaris за държавата-членка X) са:

1. Request to Core System_Request message by Client
2. Request to Other Member State_Request message by Core System of this Member State
3. Request to Core System of this Member State_Request message by Core System of other Member State
4. Request to Legacy Register_Request message by Core System
5. Request to Core System_Request message by Legacy Register
6. Response from Core System_Request message by Client
7. Response from Other Member State_Request message by Core System of this Member State
8. Response from Core System of this Member State_Request message by other Member State
9. Response from Legacy Register_Request message by Core System
10. Response from Core System_Request message by Legacy Register

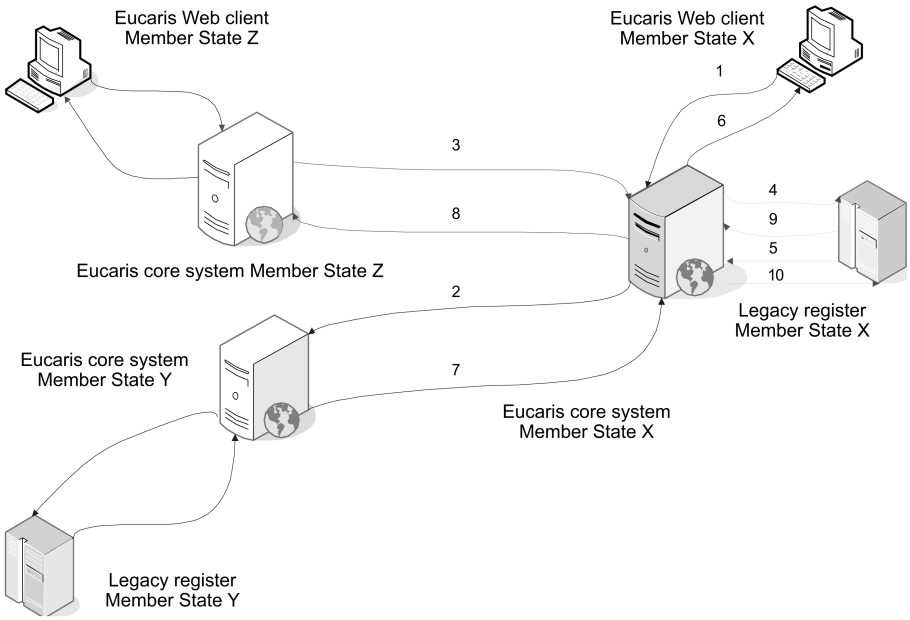
Следните видове информационен обмен са показани на фигурата:

— Искане за информация от държава-членка X до държава-членка Y — сини стрелки. Това искане и отговор се състоят съответно от съобщения вид 1, 2, 7 и 6.

— Искане за информация от държава-членка Z до държава-членка X — червени стрелки. Това искане и отговор се състоят съответно от съобщения вид 3, 4, 9 и 8.

— Искане за информация от „наследен“ местен регистър към съответната централна система (този маршрут включва и искане от „custom“ клиент, разположен зад „наследения“ регистър) — зелени стрелки. Този вид искане се състои от съобщения вид 5 и 10.

Фигура: Видове съобщения за регистриране



2.3.4. Хардуерен модул за сигурност

Не се използва хардуерен модул за сигурност.

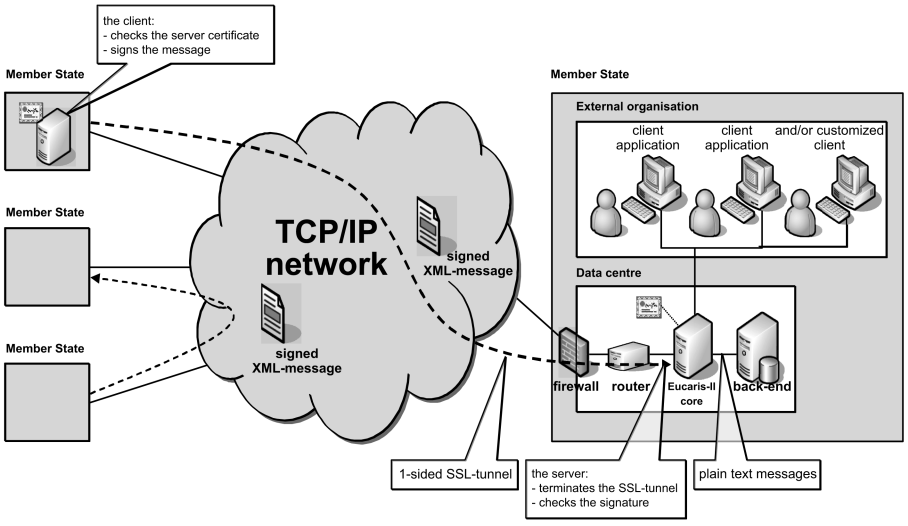
Хардуерният модул за сигурност (HSM) осигурява добра защита на ключа, който се използва за подписване на съобщенията и идентифициране на сървърите. С това се допълва цялостното ниво на сигурност, на HSM представлява висок разход за покупка/поддръжка и няма изискване за това какво решение да се вземе — за FIPS 140-2 ниво 2 или ниво 3 HSM Тъй като се използва затворена мрежа, при която заплахите се овладяват ефективно, решението е първоначално да не се използва хардуерен модул за сигурност (HSM). Ако се появи необходимост от хардуерен модул за сигурност (HSM), напр. с цел акредитация, той може да се добави към архитектурата.

3. *Технически условия на обмена на данните*

3.1. *Общо описание на приложението EUCARIS*

3.1.1. Обзорен преглед

Софтуерното приложение EUCARIS свързва всички участващи държави-членки в мрежа, в която всяка държава-членка комуникира директно с друга държава-членка. За установяване на комуникацията не е необходим централен компонент. Приложението EUCARIS се използва за защитена комуникация с другите държави-членки и за съобщения, подавани в XML-формат обратно към „наследените“ системи на държавите-членки. Тази архитектура е показана на схемата по-долу.



Държавите-членки обменят съобщения, като ги изпращат директно на получателя. Центърът за електронни данни на държавата-членка е свързан с мрежата, която се използва за обмен на съобщенията (TESTA). Държавите-членки получават достъп до мрежата TESTA посредством националния си портал за достъп до мрежата TESTA. За връзката с мрежата е необходимо да се използва firewall, а приложението Eucaris да е свързано чрез рутер с този firewall. В зависимост от избрания вариант за защита на съобщенията, се използва сертификат или от рутера, или от приложението Eucaris.

Осигурено е клиентско програмно приложение, което се използва в дадена държава-членка за търсене в собствения ѝ регистър или в регистрите на други държави-членки. Клиентското приложение се свързва с Eucaris. Клиентите се идентифицират посредством потребителско име за идентификация/парола или клиентски сертификат. Връзката с потребител във външна организация (напр. полицейска служба) може да е криптирана, но това е задължение на всяка отделна държава-членка.

3.1.2. Обхват на системата

Обхватът на системата Eucaris се ограничава до процесите, които участват в обмена на информация между органите, отговарящи за регистрацията в държавите-членки, и основните правила за представянето на тази информация. Процедурите и автоматизираните процеси, в които се използва тази информация, са извън обхвата на системата.

Държавите-членки могат да изберат да използват функционалността „Eucaris клиент“ или да си направят собствено клиентско приложение. В таблицата по-долу е описано кои аспекти на системата Eucaris се използват задължително и/или се препоръчват и кои не е задължително да се използват и/или се определят по преценка на държавата-членка.

EUCARIS aspects	M/O [1]	Remark
Network concept	M	The concept is an „any-to-any“ communication.
Physical network	M	TESTA
Core application	M	The core application of EUCARIS has to be used to connect to the other Member States. The following functionality is offered by the core: — Encrypting and signing of the messages; — Checking of the identity of the sender; — Authorization of Member States and local users; — Routing of messages; — Queuing of asynchronous messages if the recipient service is temporally unavailable; — Multiple country inquiry functionality; — Logging of the exchange of messages; — Storage of incoming messages
Client application	O	In addition to the core application the EUCARIS II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the EUCARIS organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the EUCARIS organisation and this Council Decision. The specifications can only be changed by the EUCARIS organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the EUCARIS organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

[1] M = задължително за използване или спазване, O = незадължително за използване или спазване.

3.2. *Функционални и нефункционални изисквания*

3.2.1. Обща функционалност

В този раздел се прави общо описание на общите функции.

№	Описание
1.	Системата позволява на регистрационните органите на държавите-членки да обменят съобщения с искания и отговори по интерактивен начин.
2.	Системата съдържа клиентско приложение, което позволява на крайните потребители да изпращат исканията си и да предоставят в отговор информация за ръчна обработка.
3.	Системата способства „оповестяването“, което позволява на една държава-членка да изпрати искане до всички останали държави-членки. Входящите отговори са консолидирани от централното приложение в едно съобщение отговор до клиентското приложение (тази функционалност се нарича запитване до множество страни)
4.	Системата е способна да работи с различни видове съобщения. Потребителските функции, разрешенията, маршрутизацията, подписването и регистрирането са определени поотделно за всяка категория услуги.
5.	Системата позволява на държавите членки да обменят съобщения на партиди или съобщения, които се състоят от голям брой искания или отговори. Тези съобщения се обработват асинхронно.
6.	Системата подрежда хронологично асинхронните съобщения с цел изчакване, ако получаващата държава-членка е временно неспособна да ги приеме, и гарантира доставянето им веднага след като получателят е отново на линия.
7.	Системата съхранява входящите асинхронни съобщения до момента, в който стане възможно те да бъдат обработени.
8.	Системата дава достъп единствено до приложенията Eucaris на останалите държави-членки, а не на отделни организации в рамките на тези държави-членки, т.е. всеки регистрационен орган действа като единствен портал между крайните потребители в своята държава и съответните органи в другите държави-членки.
9.	Възможно е за един Eucaris-сървър да се определят потребители от различни държави-членки, на които да се дават разрешения съгласно правата, определени в тази държава-членка.
10.	В съобщенията се дава информация за отправилата искането държава-членка и организация, както и за крайния потребител.
11.	Системата способства регистрирането на обмена на съобщения между различните държави-членки и между централното приложение и националните регистрационни системи.
12.	Системата позволява назначеният секретар — специално определена за целта организация или държава-членка — да събира регистрираната информация за съобщенията, изпратени/получени от всички участващи държави-членки с цел изготвяне на статистически отчети.
13.	Всяка държава-членка посочва самостоятелно каква регистрирана информация е предоставена на разположение на секретаря и коя информация е „само за вътрешно ползване“.
14.	Системата позволява на националните администратори на всяка държава-членка да извличат полезна статистика.
15.	Системата позволява да се добавят нови държави-членки посредством изпълнение на елементарни административни задачи.

3.2.2. Използваемост

№	Описание
16.	Системата предоставя интерфейс за автоматизирана обработка на съобщения от back-end/„наследени“ системи и позволява интегрирането на потребителския интерфейс в тези системи (customised user-interface)
17.	Системата се разбира и се усвоява лесно, като има и включени инструкции за работа в текстови формат (help-text).
18.	Системата разполага с достатъчно документация, с която подпомага държавите-членки при интегрирането, експлоатацията и поддръжката ѝ (напр. справочници, документация за функционалността и техническите характеристики, ръководство за работа и т.н.).
19.	Интерфейсът за потребителите е многоезичен и предлага възможност на крайния потребител да избере предпочитания от него език.
20.	Интерфейсът за потребителите включва компонент, чрез който местният администратор може да преведе на съответния национален език както информацията на екрана, така и кодираната информация.

3.2.3. Надеждност

№	Описание
21.	Системата е предназначена да работи като сигурна и надеждна операционна система, която е толерантна към грешките на работещите с нея и която се възстановява напълно след прекъсване на електроенергията и други аварии. Системата трябва да може да се рестартира с минимални или нулеви загуби на данни.
22.	Системата трябва да дава стабилни и възпроизводими резултати.
23.	Системата е предназначена да работи надеждно. Възможно е системата да се внедри в конфигурация, която гарантира степен на наличност 98 % (чрез повторяемост, използване на резервни (back-up) сървъри и т.н.) при всяка двустранна комуникация.
24.	Системата може да се използва частично дори при неизправност на някои компоненти (ако има авария в държавата-членка C, комуникацията между държавите-членки A и B не се прекъсва). Броят на единичните точки, в които повредата може да доведе до прекъсване на информационната верига, следва да се сведе до минимум.
25.	Времето за възстановяване след сериозна повреда следва да е по-малко от един ден. Времето, в което системата не работи, би трябвало да може да се намали максимално чрез дистанционно обслужване, напр. от център за обслужване.

3.2.4. Работни показатели

№	Описание
26.	Системата може да се използва 24 часа 7 дни в седмицата. Същият времеви диапазон (24 x 7) следователно се изисква и за „наследените“ системи на държавите-членки.
27.	Системата реагира бързо на потребителските искания независимо от извършваните „на заден план“ дейности. Същото изискване се отнася и за „наследените“ системи на страните, за да се осигури срок за реагиране в допустимите граници. Допустимият срок за реагиране на единично искане е максимум 10 секунди.
28.	Системата е проектирана за работа с множество потребители по начин, който позволява на извършваните „на заден план“ дейности да продължават докато потребителят работи „на преден план“.
29.	Системата е проектирана за мащабируемост, за да може да поддържа потенциалното увеличение на броя съобщения, когато се добавят нова функционалност или нови организации или държави-членки.

3.2.5. Сигурност

№	Описание
30.	Системата е пригодена (напр. като мерки за сигурност) за обмен на съобщения, в които се съдържат чувствителни лични данни, свързани с неприкосновеността на личния живот (напр. собственици/ ползватели на коли), класифицирана като информация за ограничено ползване в ЕС.
31.	Системата се поддържа по начин, при който не се допуска неразрешен достъп до данните.
32.	Системата включва услуга за управлението на правата и разрешенията на националните крайни потребители.
33.	На държавите-членки е осигурена възможност да проверяват самоличността на подателя (на равнище държава-членка) посредством XML-подпис.
34.	Държавите-членки трябва изрично да разрешат на друга държава-членка да иска конкретна информация.
35.	Системата предоставя на ниво приложение политика за пълна сигурност и криптиране, които са съвместими с нивото на сигурност, изисквано в подобни ситуации. В такива случаи неприкосновеността и целостта на информацията се гарантират чрез използването на XML-подписи и криптиране чрез SSL-тунелиране.
36.	Всеки обмен на съобщения може да се проследи посредством регистрирането.
37.	Предоставена е защита срещу атаки за изтриване (изтриване на съобщение от трето лице) и „прослушване“ или вмъкване („прослушване“ или изтриване на съобщение от трето лице).
38.	Системата използва сертификати на „доверени трети лица“ (TTP).
39.	Системата е способна да работи с различните сертификати на съответните държави-членки, в зависимост от вида на съобщението или услугата.

№	Описание
40.	Мерките за сигурност на ниво приложение са достатъчни, за да се осигури възможност за работа с неакредитирани мрежи.
41.	Системата е в състояние да използва основни техники за сигурност — напр. XML-firewall.

3.2.6. Приспособимост

№	Описание
42.	Системата може да се разширява, като се добавят нови видове съобщения и нова функционалност. Разходите за адаптиране са минимални поради централизираната разработка на компонентите на приложението.
43.	Държавите-членки са в състояние да дефинират нови видове съобщения за двустранно използване. Не се налага всички държави-членки да поддържат всички видове съобщения.

3.2.7. Обслужване и поддръжка

№	Описание
44.	Системата предоставя механизми за мониторинг от страна на централна служба и/или оператори по отношение на мрежата и сървърите в различните държави-членки.
45.	Системата предоставя механизми за дистанционно обслужване от централно бюро за обслужване.
46.	Системата предоставя механизми за анализ на проблемите.
47.	Системата може да се разширява, за да обхваща нови държави-членки.
48.	Приложението може лесно да се инсталира от служители с минимална квалификация и опит в областта на ИТ. Процедурата за инсталиране е автоматизирана във възможно най-голяма степен.
49.	Системата предоставя постоянна среда за провеждане на изпитвания и приемане на нови схеми.
50.	Годишните разходи за обслужване и поддръжка са намалени максимално чрез съобразяване с пазарните стандарти, като приложението е разработено по начин, който изисква възможно най-малко централно обслужване.

3.2.8. Проектни изисквания

№	Описание
51.	Системата е предназначена за продължителен експлоатационен срок и разполага със съответната документация.
52.	Системата е проектирана да работи независимо от доставчика на мрежови услуги.
53.	Системата е съвместима с действащите в държавите-членки хардуерни системи и софтуер, като взаимодейства с тези регистрационни системи посредством технология с отворен стандарт за уебуслуги (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 и т.н.).

3.2.9. Приложими стандарти

№	Описание
54.	Системата съответства на изискванията за защита на данните, изложени в Регламент (ЕО) № 45/2001 (членове 21, 22 и 23) и Директива 95/46/ЕО.
55.	Системата отговаря на стандартите на IDA.
56.	Системата поддържа UTF8.

ГЛАВА 4: **Оценяване**

1. ***Процедура за оценяване съгласно член 20 (подготовка на решения в съответствие с член 25, параграф 2 от Решение 2008/615/ПВР)***

1.1. *Въпросник*

Съответната работна група на Съвета съставя въпросник във връзка с всеки автоматизиран обмен на данни, както е посочено в глава 2 от Решение 2008/615/ПВР.

Държавата-членка попълва съответния въпросник веднага щом счете, че е изпълнила необходимите условия за дадена категория данни.

1.2. *Пилотно изпитване*

С цел оценяване на резултатите от въпросника държавата-членка, която желае да започне обмен на данни, провежда изпитване заедно с една или повече държави-членки, които вече обменят данни по решението на Съвета. Пилотното изпитване се провежда преди или скоро след посещението за оценка.

Условията и редът за пилотното изпитване ще се установят от съответната работна група на Съвета и ще се основават на предварителни, отделно сключени споразумения със съответната държава-членка. Държавите-членки, които участват в пилотното изпитване, ще вземат решение по отношение на практическите подробности.

1.3. *Посещение за оценка*

С цел оценяване на резултатите от въпросника се провежда посещение за оценка в държавата-членка, която желае да започне обмен на данни.

Условията и редът за провеждане на посещението ще се установят от съответната работна група и ще се основават на предварителни индивидуални споразумения със съответната държава-членка и екипа, който ще извърши оценката. Съответната държава-членка ще създаде условия на оценяващия екип да провери автоматизирания обмен на данни от категорията или категориите, които са предмет на оценката, по-специално като организира програмата за посещението съобразно изискванията на оценяващия екип.

В срок от един месец оценяващият екип ще изготви доклад за посещението за оценка и ще го изпрати на съответната държава-членка за коментар. Ако е уместно, оценяващият екип ще преработи този доклад въз основа на направените от държавата-членка коментари.

Оценяващият екип ще се състои от най-много трима експерти, определени от държавите-членки, участващи в автоматизирания обмен на данни за оценяваните категории данни, като тези експерти имат опит по отношение на въпросната категория данни, оправомощени са на национално равнище за работа с този вид данни и са проявили желание да участват в поне едно посещение за оценка в друга държава-членка. Комисията ще бъде поканена да се присъедини към оценяващия екип като наблюдател.

Членовете на оценяващия екип ще се съобразят с поверителния характер на информацията, която им стане известна по време на изпълнение на тази задача.

1.4. *Докладване на Съвета*

Съгласно член 25, параграф 2 от Решение 2008/615/ПВР, на Съвета се предоставя пълен доклад за оценката, в който са представени обобщено резултатите от въпросниците, посещението за оценка и пилотното изпитване.

2. ***Процедура за оценяване съгласно член 21***

2.1. *Статистика и доклад*

Всяка държава-членка ще съставя статистика относно резултатите от автоматизирания обмен на данни. За да се осигури съпоставимост, моделът за съставяне на статистиката ще се определи от съответната работна група на Съвета.

Тази статистика ще се изпраща ежегодно на генералния секретариат, който ще изготвя обобщен преглед за изтеклата година, а също и на Комисията.

Освен това, от държавите-членки ще се изисква редовно, но не по-често от веднъж годишно, да подават информация за административните, техническите и финансовите аспекти на осъществявания автоматизиран обмен на данни, която е необходима за анализиране и усъвършенстване на процеса. Въз основа на тази информация ще бъде изготвен доклад за Съвета.

2.2. *Преразглеждане*

В разумен срок Съветът ще разгледа механизма за оценяване, който е описан тук, и ще го преработи както е необходимо.

3. Експертни заседания

В рамките на съответната работна група на Съвета ще се провеждат редовни срещи на експерти с цел организирането и изпълнението на горепосочените процедури за оценяване, както и за обмен на опит и обсъждане на евентуални подобрения. При възможност, резултатите от обсъжданията на експертите ще се включват в доклада, посочен в точка 2.1 по-горе.

РЕШЕНИЕ 2008/617/ПВР НА СЪВЕТА

от 23 юни 2008 година

за подобряване на сътрудничеството между групите за специална намеса на държавите-членки на Европейския съюз в кризисни ситуации

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за Европейския съюз, и по-специално членове 30 и 32 и член 34, параграф 2, буква в) от него,

като взе предвид инициативата на Република Австрия ([1]),

като взе предвид становището на Европейския парламент ([2]),

като има предвид, че:

(1) Съгласно член 29 от Договора Съюзът има за цел да предоставя на гражданите високо равнище на закрила в рамките на пространство на свобода, сигурност и правосъдие чрез развиването на съвместна дейност между държавите-членки в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси.

(2) В Декларацията си относно солидарността в борбата с тероризма от 25 март 2004 г. държавните и правителствените ръководители на държавите-членки на Европейския съюз заявиха твърдото си намерение да мобилизират всички инструменти, с които разполагат, за подпомагането на държава-членка или присъединяваща се държава, на нейна територия, по молба на нейните политически власти, в случай на терористична атака.

(3) След нападенията от 11 септември 2001 г. групите за специална намеса на всички правоохранителни органи на държавите-членки вече са започнали дейности по сътрудничество под егидата на оперативната група на полицейските началници. От 2001 г. тяхната мрежа, наречена „Атлас“, е провела различни семинари, проучвания, обмен на материали и съвместни учения.

(4) Нито една държава-членка не разполага с всички средства, ресурси и експертни знания за ефективно справяне с всички възможни видове конкретни или широкомащабни кризисни ситуации, които изискват специална намеса. Следователно е жизненоважно всяка държава-членка да може да поиска съдействие от друга държава-членка.

(5) Решение на Съвета 2008/615/ПВР от 23 юни 2008 г. за засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност ([3]) („Решението от Прюм“), и по-конкретно член 18 от него, урежда формите на полицейско съдействие между държавите-членки във връзка с масови събирания и подобни големи събития, бедствия и сериозни произшествия. Настоящото решение не обхваща масовите събирания, природните бедствия или сериозните произшествия по смисъла на член 18 от Решението от Прюм, но допълва онези разпоредби на Решението от Прюм, които предвиждат форми на полицейско съдействие между държавите-членки чрез групи за специална намеса в други ситуации, а именно в кризисни ситуации, предизвикани от човешко поведение, които представляват сериозна пряка физическа заплаха за хора, имущество, инфраструктура или институции, по-специално вземане на заложници, отвличания и подобни събития.

(6) Наличието на настоящата правна рамка и на списък на компетентните органи ще позволи на държавите-членки да реагират бързо и да печелят време, ако възникне такава кризисна ситуация. Нещо повече, с оглед увеличаване на способността на държавите-членки да предотвратяват и да отговарят на такива кризисни ситуации и по-специално на терористични актове, е особено важно групите за специална намеса да се срещат редовно и да организират съвместни обучения, за да се възползват взаимно от опита си,

РЕШИ:

Член 1

Предмет

Настоящото решение установява общите правила и условия, които позволяват на групите за специална намеса на една държава-членка да оказват съдействие и/или да действат на територията на друга държава-членка (наричана по-долу „молеща държава-членка“) в случаите, в които те са били поканени от молещата държава-членка и са се съгласили да направят това с цел справяне с кризисна ситуация. Практическите подробности и разпоредбите за изпълнение, които допълват настоящото решение, се договарят пряко между молещата държава-членка и помолената държава-членка.

Член 2

Определения

За целите на настоящото решение:

а) „група за специална намеса“ означава всяко правоохранително звено на държава-членка, което е специализирано в областта на контрола на кризисни ситуации;

([1]) ОВ C 321, 29.12.2006 г., стр. 45.

([2]) Становище от 31 януари 2008 г. (все още непубликувано в Официален вестник).

([3]) Вж. страница 1 от настоящия брой на Официален вестник.

б) „кризисна ситуация“ означава всяка ситуация, при която компетентните органи на държава-членка имат основателни причини да вярват, че е налице престъпление, което представлява сериозна пряка физическа заплаха за хора, имущество, инфраструктура или институции в тази държава-членка, по-специално ситуациите, посочени в член 1, параграф 1 от Рамково решение 2002/475/ПВР на Съвета от 13 юни 2002 г. относно борбата срещу тероризма ([1]);

в) „компетентен орган“ означава националния орган, който може да отправя молби и да предоставя разрешения за разполагането на групи за специална намеса.

Член 3

Съдействие за друга държава-членка

1. Посредством молба чрез компетентните органи, в която се посочва характерът на поисканото съдействие, както и оперативната необходимост от такава, държава-членка може да поиска да бъде подпомогната от група за специална намеса на друга държава-членка с оглед преодоляването на кризисна ситуация. Компетентният орган на помолената държава-членка може да приеме или да отхвърли тази молба, или да предложи различен вид съдействие.

2. При наличие на споразумение между съответните държави-членки съдействието може да се изразява в предоставяне на молещата държава-членка на оборудване и/или на експертни знания, и/или на извършване на действия на територията на тази държава-членка, като при необходимост се използват оръжия.

3. В случай на действия на територията на молещата държава-членка служителите на подпомагащата група за специална намеса са оправомощени да действат в качеството си на подпомагащи на територията на молещата държава-членка и да предприемат всички необходими мерки, за да предоставят поисканото съдействие, доколкото те:

а) действат с разрешението, под контрола и ръководството на молещата държава-членка и в съответствие с правото на молещата държава-членка; и

б) действат в границите на правомощията, с които разполагат по националното си законодателство.

Член 4

Гражданска и наказателна отговорност

Когато служители на една държава-членка действат в друга държава-членка и/или оборудването им се използва съгласно настоящото решение, се прилагат разпоредбите относно гражданската и наказателната отговорност, изложени в член 21, параграфи 4 и 5 и член 22 от Решението от Прюм.

([1]) ОВ L 164, 22.6.2002 г., стр. 3.

Член 5

Срещи и съвместно обучение

Участващите държавите-членки следят техните групи за специална намеса да провеждат срещи и да организират съвместни обучения и учения, при необходимост, с цел обмяна на опит, експертни знания и обща, практическа и техническа информация относно справянето с кризисна ситуация. Тези срещи, обучения и учения могат да бъдат финансирани по линия на възможностите, предлагани от финансовите програми на Съюза за получаване на безвъзмездни средства от бюджета на Европейския съюз. В този контекст държавата-членка, която осигурява председателството на Съюза, се стреми да осигури провеждането на такива срещи, обучения и учения.

Член 6

Разходи

Молещата държава-членка поема оперативните разходи, направени от групите за специална намеса на помолената държава-членка във връзка с прилагането на член 3, включително разходите за транспорт и настаняване, освен ако между съответните държави-членки е договорено друго.

Член 7

Отношение с други инструменти

1. Без да се засягат задълженията им по други актове, приети съгласно дял VI от Договора, и по-специално Решението от Прюм:

а) държавите-членки могат да продължат да прилагат двустранни или многостранни споразумения или договорености за трансгранично сътрудничество, които са в сила към 23 юни 2008 г., доколкото подобни споразумения или договорености не са несъвместими с целите на настоящото решение;

б) държавите-членки могат да сключват или въвеждат в сила двустранни или многостранни споразумения или договорености за трансгранично сътрудничество след 23 декември 2008 г., доколкото подобни споразумения или договорености предвиждат доразвиване или разгръщане на целите на настоящото решение.

2. Споразуменията и договореностите, посочени в параграф 1, не може да засягат взаимоотношенията с държави-членки, които не са страни по тях.

3. Държавите-членки информират Съвета и Комисията за споразуменията или договореностите, посочени в параграф 1.

Член 8

Заключителни разпоредби

Генералният секретариат на Съвета съставя и актуализира списъка с компетентни органи на държавите-членки, които могат да отправят молби и да предоставят разрешенията за оказване на съдействие, посочени в член 3.

Генералният секретариат на Съвета информира органите, посочени в параграф 1, за всички промени в списъка, създаден съгласно настоящия член.

Член 9

Влизане в сила

Настоящото решение влиза в сила на 23 декември 2008 г.

Съставено в Люксембург на 23 юни 2008 година.

За Съвета

Председател

I. JARC