DECYZJA RADY 2008/616/WSiSW

z dnia 23 czerwca 2008 r.

w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej

RADA UNII EUROPEJSKIEJ,

uwzględniając art. 33 decyzji Rady 2008/615/WSiSW ([1]),

uwzględniając inicjatywę Republiki Federalnej Niemiec,

uwzględniając opinię Parlamentu Europejskiego ([2]),

a także mając na uwadze, co następuje:

(1) W dniu 23 czerwca 2008 r. Rada przyjęła decyzję 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej.

(2) Na mocy decyzji 2008/615/WSiSW do systemu uregulowań prawnych Unii Europejskiej przeniesiono podstawowe elementy konwencji z dnia 27 maja 2005 r. zawartej między Królestwem Belgii, Republiką Federalną Niemiec, Królestwem Hiszpanii, Republiką Francuską, Wielkim Księstwem Luksemburga, Królestwem Niderlandów i Republiką Austrii w sprawie intensyfikacji współpracy transgranicznej, szczególnie w walce z terroryzmem, przestępczością transgraniczną i nielegalną migracją (zwanej dalej „konwencją z Prüm").

(3) W art. 33 decyzji 2008/615/WSiSW przewiduje się przyjęcie przez Radę środków niezbędnych do wdrożenia decyzji 2008/615/WSiSW na szczeblu Unii, zgodnie z procedurą określoną w art. 34 ust. 2 lit. c) zdanie drugie Traktatu o Unii Europejskiej. Środki te mają się opierać na porozumieniu wykonawczym z dnia 5 grudnia 2006 r. dotyczącym administracyjnych i technicznych aspektów wprowadzania w życie i stosowania konwencji z Prüm.

(4) W niniejszej decyzji ustala się wspólne przepisy normatywne niezbędne do administracyjnej i technicznej realizacji form współpracy przedstawionych w decyzji 2008/615/WSiSW. W załączniku do niniejszej decyzji zamieszczono przepisy wykonawcze o charakterze technicznym. Ponadto Sekretariat Generalny Rady sporządzi i będzie aktualizował osobny podręcznik zawierający wyłącznie faktyczne informacje, których mają dostarczyć państwa członkowskie.

(5) Ze względu na możliwości techniczne rutynowe przeszukania nowych profili DNA zasadniczo będą przeprowadzane w formie pojedynczych przeszukań, a odpowiednie rozwiązania zostaną opracowane na szczeblu technicznym,

([1]) Zob. s. 1 niniejszego Dziennika Urzędowego.

([2]) Opinia z dnia 21 kwietnia 2008 r. (dotychczas nieopublikowana w Dzienniku Urzędowym).

STANOWI, CO NASTĘPUJE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Cel

Celem niniejszej decyzji jest ustanowienie niezbędnych przepisów administracyjnych i technicznych w celu wdrożenia decyzji 2008/615/WSiSW, w szczególności w odniesieniu do zautomatyzowanej wymiany danych DNA, danych daktyloskopijnych oraz danych rejestracyjnych pojazdów, określonej w rozdziale 2 tej decyzji, oraz w odniesieniu do innych form współpracy określonych w rozdziale 5 tej decyzji.

Artykuł 2

Definicje

Na użytek niniejszej decyzji:

a) „przeszukanie" i „porównanie", o których mowa w art. 3, 4 i 9 decyzji 2008/615/WSiSW, oznaczają procedury, poprzez które ustala się istnienie zgodności między danymi DNA lub danymi daktyloskopijnymi przekazanymi przez jedno państwo członkowskie a danymi DNA lub danymi daktyloskopijnymi przechowywanymi w bazach danych innego państwa członkowskiego, kilku z nich lub wszystkich państw członkowskich;

b) „zautomatyzowane przeszukanie", o którym mowa w art. 12 decyzji 2008/615/WSiSW, oznacza procedurę dostępu *on-line* służącą przeglądowi baz danych jednego państwa członkowskiego, kilku z nich lub wszystkich państw członkowskich;

c) „profil DNA" oznacza literę lub kod numeryczny reprezentujące charakterystyczne cechy identyfikacyjne niekodującej części przeanalizowanej próbki ludzkiego DNA, tj. szczególną strukturę molekularną w różnych loci DNA;

d) „niekodująca część DNA" oznacza części chromosomów niemające wartości genetycznej, tj. takie, o których nie wiadomo, by odpowiadały jakimkolwiek funkcjonalnym właściwościom organizmu;

e) „dane referencyjne DNA" oznaczają profil DNA oraz oznaczenie referencyjne;

f) „referencyjny profil DNA" oznacza profil DNA pochodzący od zidentyfikowanej osoby;

g) „niezidentyfikowany profil DNA" oznacza profil DNA uzyskany ze śladów zebranych podczas dochodzenia w sprawie przestępstwa i należący do dotychczas niezidentyfikowanej osoby;

h) „notatka" oznacza zaznaczenie przez dane państwo członkowskie na profilu DNA znajdującym się w jego bazie danych, że stwierdzono już zgodność tego profilu z informacjami uzyskanymi w wyniku przeszukania lub porównania przez inne państwo członkowskie;

i) „dane daktyloskopijne" oznaczają obrazy odbitek linii papilarnych palców, obrazy śladów palców, odbitek dłoni, śladów dłoni oraz wzory takich obrazów (zakodowane minucje), gdy są one przechowywane i przetwarzane w zautomatyzowanej bazie danych;

j) „dane rejestracyjne pojazdów" oznaczają zbiór danych określony w rozdziale 3 załącznika do niniejszej decyzji;

k) „pojedynczy przypadek", o którym mowa w art. 3 ust. 1 zdanie drugie, w art. 9 ust. 1 zdanie drugie i w art. 12 ust. 1 decyzji 2008/615/WSiSW, oznacza pojedyncze dochodzenie lub akta prokuratorskie. Jeżeli akta te zawierają więcej niż jeden profil DNA, jeden komplet danych daktyloskopijnych lub danych rejestracyjnych pojazdu, mogą one zostać przekazane razem jako jedno zapytanie.

ROZDZIAŁ 2

WSPÓLNE PRZEPISY DOTYCZĄCE WYMIANY DANYCH

Artykuł 3

Specyfikacje techniczne

Państwa członkowskie stosują wspólne specyfikacje techniczne przy wszelkich zapytaniach i odpowiedziach związanych z przeszukaniem i porównaniem profili DNA, danych daktyloskopijnych i danych rejestracyjnych pojazdów. Wspomniane specyfikacje techniczne są zawarte w załączniku do niniejszej decyzji.

Artykuł 4

Sieć łączności

Elektroniczna wymiana danych DNA, danych daktyloskopijnych oraz danych rejestracyjnych pojazdów między państwami członkowskimi odbywa się z wykorzystaniem transeuropejskiej sieci teleinformatycznej do wymiany danych pomiędzy jednostkami administracyjnymi (TESTA II) oraz jej kolejnych wersji.

Artykuł 5

Dostępność zautomatyzowanej wymiany danych

Państwa członkowskie podejmują wszelkie niezbędne środki w celu zapewnienia, aby zautomatyzowane przeszukanie lub porównanie danych DNA, danych daktyloskopijnych i danych rejestracyjnych pojazdów było możliwe przez całą dobę i cały tydzień. W przypadku awarii technicznej krajowe punkty kontaktowe państw członkowskich niezwłocznie informują się o tym nawzajem i uzgadniają tymczasowe sposoby wymiany danych zgodne z obowiązującymi przepisami. Zautomatyzowana wymiana danych jest przywracana możliwie jak najszybciej.

Artykuł 6

Oznaczenia referencyjne danych DNA i danych daktyloskopijnych

Oznaczenia referencyjne, o których mowa w art. 2 i 8 decyzji 2008/615/WSiSW, składają się z połączenia następujących oznaczeń:

a) kodu, który w przypadku stwierdzenia zgodności umożliwia państwom członkowskim pozyskanie danych osobowych i innych informacji znajdujących się w ich bazach danych i przekazanie ich do jednego państwa członkowskiego, kilku z nich lub wszystkich państw członkowskich, zgodnie z art. 5 lub art. 10 decyzji 2008/615/WSiSW;

b) kodu oznaczającego pochodzenie krajowe profilu DNA lub danych daktyloskopijnych; oraz

c) w odniesieniu do danych DNA, kodu oznaczającego rodzaj profilu DNA.

ROZDZIAŁ 3

DANE DNA

Artykuł 7

Zasady wymiany danych DNA

1. Państwa członkowskie korzystają z istniejących norm wymiany danych DNA, takich jak Europejski Standardowy Zestaw Loci (ESS) lub Standardowy Zestaw Loci Interpolu (ISSOL).

2. W przypadku zautomatyzowanego przeszukania i porównania profili DNA procedura transmisji odbywa się w ramach struktury zdecentralizowanej.

3. Stosuje się odpowiednie środki w celu zapewnienia poufności i integralności danych przekazywanych innym państwom członkowskim, w tym szyfrowanie danych.

4. Państwa członkowskie stosują środki niezbędne do zagwarantowania integralności profili DNA udostępnianych lub przesyłanych do innych państw członkowskich celem porównania i zapewniają zgodność tych środków z normami międzynarodowymi, takimi jak ISO 17025.

5. Państwa członkowskie stosują kody państw członkowskich zgodnie z normą ISO 3166-1 alfa-2.

Artykuł 8

Zasady dotyczące zapytań i odpowiedzi związanych z danymi DNA

1. Zapytanie dotyczące zautomatyzowanego przeszukania lub porównania, o których mowa w art. 3 lub 4 decyzji 2008/615/WSiSW, zawiera jedynie następujące informacje:

a) kod zapytującego państwa członkowskiego;

b) datę, godzinę i numer zapytania;

c) profile DNA i ich oznaczenia referencyjne;

d) rodzaje przekazywanych profili DNA (niezidentyfikowane lub referencyjne profile DNA); oraz

e) informacje wymagane do kontrolowania systemów baz danych i kontroli jakości automatycznego procesu przeszukiwania.

2. Odpowiedź na zapytanie (wynik porównania), o którym mowa w ust. 1, zawiera jedynie następujące informacje:

a) wskazanie, czy stwierdzono zgodność danych (ile razy) lub nie;

b) datę, godzinę i numer zapytania;

c) datę, godzinę i numer odpowiedzi;

d) kody zapytującego i zapytanego państwa członkowskiego;

e) oznaczenia referencyjne zapytującego i zapytanego państwa członkowskiego;

f) rodzaje przekazywanych profili DNA (niezidentyfikowane lub referencyjne profile DNA);

g) żądane i zgodne profile DNA; oraz

h) informacje wymagane do kontrolowania systemów baz danych i kontroli jakości automatycznego procesu przeszukiwania.

3. Zautomatyzowane powiadomienie o zgodności jest przekazywane jedynie wtedy, gdy wynikiem zautomatyzowanego przeszukania lub porównania jest zgodność minimalnej liczby loci. Ta minimalna liczba określona jest w rozdziale 1 załącznika do niniejszej decyzji.

4. Państwa członkowskie zapewniają zgodność swoich zapytań z oświadczeniami wydanymi na podstawie art. 2 ust. 3 decyzji 2008/615/WSiSW. Oświadczenia te zostają przedstawione w podręczniku, o którym mowa w art. 18 ust. 2 niniejszej decyzji.

Artykuł 9

Procedura transmisji przy zautomatyzowanym przeszukaniu niezidentyfikowanych profili DNA zgodnie z art. 3 decyzji 2008/615/WSiSW

1. Jeżeli w trakcie przeszukania nie stwierdzono zgodności posiadanego niezidentyfikowanego profilu DNA z informacjami znajdującymi się w krajowej bazie danych lub stwierdzono zgodność z niezidentyfikowanym profilem DNA, profil ten można następnie przekazać do wszystkich baz danych innych państw członkowskich, a jeżeli w trakcie tego przeszukania stwierdzono zgodność tego niezidentyfikowanego profilu DNA z referencyjnymi lub niezidentyfikowanymi profilami DNA znajdującymi się w bazach danych innych państw członkowskich, to automatycznie powiadamia się o zgodności zapytujące państwo członkowskie i przekazuje mu się dane referencyjne DNA; jeżeli nie stwierdzono zgodności z informacjami znajdującymi się w bazach danych innych państw członkowskich, automatycznie powiadamia się o tym zapytujące państwo członkowskie.

2. Jeżeli w trakcie przeszukania stwierdzono zgodność posiadanego niezidentyfikowanego profilu DNA z informacjami znajdującymi się w bazach danych innych państw członkowskich, każde odnośne państwo członkowskie może wprowadzić odpowiednią notatkę do krajowej bazy danych.

Artykuł 10

Procedura transmisji przy zautomatyzowanym przeszukaniu referencyjnych profili DNA zgodnie z art. 3 decyzji 2008/615/WSiSW

Jeżeli w trakcie przeszukania nie stwierdzono zgodności posiadanego referencyjnego profilu DNA z informacjami znajdującymi się w krajowej bazie danych lub jeżeli stwierdzono zgodność z niezidentyfikowanym profilem DNA, dany referencyjny profil DNA można następnie przekazać do wszystkich baz danych innych państw członkowskich, a jeżeli w trakcie przeszukania stwierdzono zgodność posiadanego referencyjnego profilu DNA z referencyjnymi lub niezidentyfikowanymi profilami DNA znajdującymi się w bazach danych innych państw członkowskich, to automatycznie powiadamia się o zgodności zapytujące państwo członkowskie i przekazuje mu się dane referencyjne DNA; jeżeli nie stwierdzono zgodności z informacjami znajdującymi się w bazach danych innych państw członkowskich, automatycznie powiadamia się o tym zapytujące państwo członkowskie.

Artykuł 11

Procedura transmisji przy zautomatyzowanym porównaniu niezidentyfikowanych profili DNA zgodnie z art. 4 decyzji 2008/615/WSiSW

1. Jeżeli w trakcie porównania stwierdzono zgodność posiadanych niezidentyfikowanych profili DNA z referencyjnymi lub niezidentyfikowanymi profilami DNA znajdującymi się w bazach danych innych państw członkowskich, to automatycznie powiadamia się o zgodności zapytujące państwo członkowskie i przekazuje mu się dane referencyjne DNA.

2. Jeżeli w trakcie porównania stwierdzono zgodność posiadanych niezidentyfikowanych profili DNA z niezidentyfikowanymi lub referencyjnymi profilami DNA znajdującymi się w bazach danych innych państw członkowskich, każde odnośne państwo członkowskie może wprowadzić odpowiednią notatkę do krajowej bazy danych.

ROZDZIAŁ 4

DANE DAKTYLOSKOPIJNE

Artykuł 12

Zasady wymiany danych daktyloskopijnych

1. Przekształcenie danych daktyloskopijnych w formę cyfrową i ich przekazanie do innych państw członkowskich przeprowadza się zgodnie z ujednoliconym formatem danych określonym w rozdziale 2 załącznika do niniejszej decyzji.

2. Każde państwo członkowskie zapewnia odpowiednią jakość przekazywanych przez siebie danych daktyloskopijnych, umożliwiającą ich porównanie za pomocą automatycznego systemu identyfikacji daktyloskopijnej (AFIS).

3. Procedura transmisji danych przy wymianie danych daktyloskopijnych odbywa się w ramach struktury zdecentralizowanej.

4. W celu zapewnienia poufności i integralności danych daktyloskopijnych przekazywanych innym państwom członkowskim stosuje się odpowiednie środki, w tym szyfrowanie danych.

5. Państwa członkowskie stosują kody państw członkowskich zgodnie z normą ISO 3166-1 alfa-2.

Artykuł 13

Możliwości przeszukania danych daktyloskopijnych

1. Każde państwo członkowskie zapewnia, aby jego zapytania dotyczące przeszukania nie przekraczały możliwości przeszukania określonych przez zapytane państwo członkowskie. Państwa członkowskie przekazują Sekretariatowi Generalnemu Rady oświadczenia, o których mowa w art. 18 ust. 2 i w których określają maksymalne dzienne możliwości przeszukania danych daktyloskopijnych osób zidentyfikowanych i dotychczas niezidentyfikowanych.

2. Maksymalna liczba osób, których dane można jednocześnie przekazać do weryfikacji, jest określona w rozdziale 2 załącznika do niniejszej decyzji.

Artykuł 14

Zasady dotyczące zapytań i odpowiedzi związanych z danymi daktyloskopijnymi

1. Zapytane państwo członkowskie bezzwłocznie sprawdza w sposób w pełni zautomatyzowany jakość przekazanych danych daktyloskopijnych. Jeśli dane nie nadają się do zautomatyzowanego porównania, zapytane państwo członkowskie bezzwłocznie informuje o tym zapytujące państwo członkowskie.

2. Zapytane państwo członkowskie prowadzi przeszukania w takiej kolejności, w jakiej otrzymuje zapytania. Zapytania przetwarza się w sposób w pełni zautomatyzowany w ciągu 24 godzin. Zapytujące państwo członkowskie może zwrócić się o zastosowanie przyspieszonego trybu przetwarzania jego zapytań, jeżeli jest to przewidziane w prawie krajowym, a wtedy zapytane państwo członkowskie bezzwłocznie przeprowadza przeszukania. Jeżeli terminów nie można dotrzymać z racji siły wyższej, porównanie przeprowadza się bezzwłocznie, gdy tylko zostaną usunięte przeszkody.

ROZDZIAŁ 5

DANE REJESTRACYJNE POJAZDÓW

Artykuł 15

Zasady zautomatyzowanego przeszukania danych rejestracyjnych pojazdów

1. Do zautomatyzowanego przeszukania danych rejestracyjnych pojazdów państwa członkowskie wykorzystują wersję oprogramowania europejskiego systemu informacji o pojazdach i prawach jazdy (EUCARIS) specjalnie zaprojektowaną do celów art. 12 decyzji 2008/615/WSiSW oraz poprawione wersje tego oprogramowania.

2. Zautomatyzowane przeszukanie danych rejestracyjnych pojazdów odbywa się w ramach struktury zdecentralizowanej.

3. Informacje wymieniane za pośrednictwem systemu EUCARIS są przekazywane w formie zaszyfrowanej.

4. Elementy danych rejestracyjnych pojazdów podlegające wymianie są określone w rozdziale 3 załącznika do niniejszej decyzji.

5. Przy wykonywaniu przepisów art. 12 decyzji 2008/615/WSiSW państwa członkowskie mogą nadać rangę priorytetową przeszukaniom związanym ze zwalczaniem poważnej przestępczości.

Artykuł 16

Koszty

Każde państwo członkowskie ponosi koszty powstałe w wyniku administrowania, użytkowania i konserwacji oprogramowania EUCARIS, o którym mowa w art. 15 ust. 1.

ROZDZIAŁ 6

WSPÓŁPRACA POLICYJNA

Artykuł 17

Wspólne patrole i inne wspólne operacje

1. Zgodnie z przepisami rozdziału 5 decyzji 2008/615/WSiSW, w szczególności z oświadczeniami przekazanymi na mocy jej art. 17 ust. 4 oraz art. 19 ust. 2 i 4 tej decyzji, każde państwo członkowskie wyznacza co najmniej jeden punkt

kontaktowy, pozwalający innym państwom członkowskim zwrócić się do właściwych organów, oraz może określić własne procedury ustanawiania wspólnych patroli i przeprowadzania innych wspólnych operacji, procedury dotyczące inicjatyw innych państw członkowskich w odniesieniu do tych operacji oraz pozostałe związane z tymi operacjami aspekty praktyczne i metody działania.

2. Sekretariat Generalny Rady sporządza i aktualizuje wykaz punktów kontaktowych i informuje właściwe organy o wszelkich zmianach w tym wykazie.

3. Z inicjatywą przeprowadzenia wspólnej operacji mogą wystąpić właściwe organy każdego państwa członkowskiego. Przed rozpoczęciem danej operacji właściwe organy, o których mowa w ust. 2, dokonują pisemnych lub ustnych ustaleń, w których można określić szczegóły, takie jak:

a) właściwe organy każdego państwa członkowskiego w odniesieniu do operacji;

b) konkretny cel operacji;

c) przyjmujące państwo członkowskie, w którym operacja ma miejsce;

d) obszar geograficzny przyjmującego państwa członkowskiego, w którym operacja ma miejsce;

e) okres objęty operacją;

f) konkretna pomoc, jakiej przyjmującemu państwu członkowskiemu ma udzielić wysyłające państwo lub państwa członkowskie, obejmująca funkcjonariuszy lub innych pracowników, aspekty materialne i finansowe;

g) funkcjonariusze uczestniczący w operacji;

h) funkcjonariusz odpowiedzialny za operację,

i) uprawnienia, jakie przysługują funkcjonariuszom i innym pracownikom pochodzącym z wysyłającego państwa członkowskiego lub z wysyłających państw członkowskich podczas operacji w przyjmującym państwie członkowskim;

j) konkretna broń, amunicja i sprzęt, z których podczas operacji mogą korzystać wysłani funkcjonariusze zgodnie z decyzją 2008/615/WSiSW;

k) aspekt logistyczny działań w odniesieniu do transportu, zakwaterowania i bezpieczeństwa;

l) podział kosztów wspólnej operacji, jeżeli jest inny, niż określono w art. 34 zdanie pierwsze decyzji Rady 2008/615/WSiSW;

m) wszelkie inne wymagane elementy.

4. Oświadczenia, procedury i wyznaczenia przewidziane w niniejszym artykule zostaną przedstawione w podręczniku, o którym mowa w art. 18 ust. 2.

ROZDZIAŁ 7

PRZEPISY KOŃCOWE

Artykuł 18

Załącznik i podręcznik

1. Dalsze szczegóły dotyczące technicznego i administracyjnego aspektu wdrażania decyzji 2008/615/WSiSW są przedstawione w załączniku do niniejszej decyzji.

2. Sekretariat Generalny Rady sporządza i aktualizuje podręcznik zawierający wyłącznie faktyczne informacje przekazane przez państwa członkowskie w oświadczeniach złożonych zgodnie z decyzją 2008/615/WSiSW lub z niniejszą decyzją lub w drodze powiadomień przekazanych Sekretariatowi Generalnemu Rady. Podręcznik ma formę dokumentu Rady.

Artykuł 19

Niezależne organy ochrony danych

Zgodnie z art. 18 ust. 2 niniejszej decyzji państwa członkowskie informują Sekretariat Generalny Rady o niezależnych organach ochrony danych lub organach sądowych, o których mowa w art. 30 ust. 5 decyzji 2008/615/WSiSW.

Artykuł 20

Przygotowanie decyzji, o których mowa w art. 25 ust. 2 decyzji 2008/615/WSiSW

1. Rada podejmuje decyzję, o której mowa w art. 25 ust. 2 decyzji 2008/615/WSiSW, na podstawie sprawozdania z oceny opartego na kwestionariuszu.

2. W odniesieniu do zautomatyzowanej wymiany danych zgodnie z rozdziałem 2 decyzji Rady 2008/615/WSiSW sprawozdanie z oceny jest również oparte na wynikach wizyty ewaluacyjnej oraz operacji pilotażowej, które zostaną przeprowadzone wówczas, gdy odpowiednie państwo członkowskie przekaże Sekretariatowi Generalnemu informacje zgodnie z art. 36 ust. 2 zdanie pierwsze decyzji 2008/615/WSiSW.

3. Dalsze szczegóły tej procedury są określone w rozdziale 4 załącznika do niniejszej decyzji.

Artykuł 21

Ocena wymiany danych

1. Przeprowadza się regularną ocenę aspektów administracyjnych, technicznych i finansowych stosowania wymiany danych zgodnie z rozdziałem 2 decyzji 2008/615/WSiSW, a w szczególności stosowania mechanizmu przedstawionego w art. 15 ust. 5. Ocena dotyczy tych państw członkowskich, które stosują decyzję 2008/615/WSiSW w chwili przeprowadzenia oceny, i dotyczy tych kategorii danych, które zaczęły podlegać wymianie między

danymi państwami członkowskimi. Ocena jest oparta na sprawozdaniach odpowiednich państw członkowskich.

2. Dalsze szczegóły tej procedury są określone w rozdziale 4 załącznika do niniejszej decyzji.

Artykuł 22

Związek z porozumieniem wykonawczym do konwencji z Prüm

Do państw członkowskich związanych postanowieniami konwencji z Prüm mają zastosowanie odpowiednie przepisy niniejszej decyzji i załącznika do niej, po ich całkowitym wdrożeniu, zamiast odpowiadających tym przepisom postanowień zawartych w porozumieniu wykonawczym do konwencji z Prüm. Wszelkie pozostałe postanowienia porozumienia wykonawczego pozostają w mocy między umawiającymi się stronami konwencji z Prüm.

Artykuł 23

Wykonanie

Państwa członkowskie podejmują wszelkie środki konieczne do realizacji przepisów niniejszej decyzji w terminach określonych w art. 36 ust. 1 decyzji 2008/615/WSiSW.

Artykuł 24

Stosowanie

Niniejsza decyzja staje się skuteczna dwadzieścia dni po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Luksemburgu dnia 23 czerwca 2008 r.

W imieniu Rady

I. JARC

Przewodniczący

ZAŁĄCZNIK

SPIS TREŚCI

ROZDZIAŁ 1: **Wymiana danych DNA**

1. ***Kwestie z dziedziny medycyny sądowej związane z DNA, zasady i algorytmy zgodności***

1.1. *Właściwości profili DNA*

1.2. *Zasady ustalania zgodności*

1.3. *Zasady sprawozdawczości*

2. ***Tabela kodów państw członkowskich***

3. ***Analiza funkcjonalna***

3.1. *Dostępność systemu*

3.2. *Drugi krok*

4. ***Dokument kontroli interfejsu DNA***

4.1. *Wstęp*

4.2. *Definicja struktury XML*

5. ***Architektura aplikacji, bezpieczeństwa i komunikacji***

5.1. *Zarys*

5.2. *Architektura górnego szczebla*

5.3. *Normy bezpieczeństwa i ochrona danych*

5.4. *Protokoły i normy, które mają być wykorzystywane do szyfrowania*

5.5. *Architektura aplikacji*

5.6. *Protokoły i normy, które mają być wykorzystywane w architekturze aplikacji*

5.7. *Środowisko komunikacyjne*

ROZDZIAŁ 2: **Wymiana danych daktyloskopijnych (dokument kontroli interfejsu)**

1. ***Zarys zawartości plików***

2. ***Format rekordu***

3. ***Rekord logiczny typu 1: nagłówek pliku***

4. ***Rekord logiczny typu 2: tekst opisu***

5. ***Rekord logiczny typu 4: obraz o wysokiej rozdzielczości w odcieniach szarości***

6. ***Rekord logiczny typu 9: zapis minucji***

7. ***Rekord typu 13: obraz śladu, o zmiennej rozdzielczości***

8. ***Rekord typu 15: obraz odbitki dłoni, o zmiennej rozdzielczości***

9. ***Dodatki do rozdziału 2***

9.1. *Kody separatora ASCII*

9.2. *Obliczanie kontrolnych znaków alfa-numerycznych*

9.3. *Kody znaków*

9.4. *Streszczenie transakcji*

9.5. *Definicje rekordów typu 1*

9.6. *Definicje rekordów typu 2*

9.7. *Kody kompresji odcieni szarości*

9.8. *Specyfikacja poczty*

ROZDZIAŁ 3: **Wymiana danych rejestracyjnych pojazdów**

1. ***Wspólny zestaw danych do zautomatyzowanego przeszukania danych rejestracyjnych pojazdów***

1.1. *Definicje*

1.2. *Poszukiwanie właściciela/posiadacza pojazdu*

2. ***Bezpieczeństwo danych***

2.1. *Zarys*

2.2. *Aspekty bezpieczeństwa dotyczące wymiany wiadomości*

2.3. *Aspekty bezpieczeństwa niedotyczące wymiany wiadomości*

3. ***Warunki techniczne wymiany danych***

3.1. *Ogólny opis oprogramowania EUCARIS*

3.2. *Wymogi funkcjonalne i inne*

ROZDZIAŁ 4: **Ocena**

1. ***Procedura oceny zgodnie z art. 20 (opracowanie decyzji zgodne z art. 25 ust. 2 decyzji 2008/615/WSiSW)***

1.1. *Procedura*

1.2. *Operacja pilotażowa*

1.3. *Inspekcja*

1.4. *Sprawozdanie dla Rady*

2. ***Procedura oceny zgodnie z art. 21***

2.1. *Dane statystyczne i sprawozdanie*

2.2. *Korekta*

3. ***Spotkania ekspertów***

ROZDZIAŁ 1: **Wymiana danych DNA**

1. ***Kwestie z dziedziny medycyny sądowej związane z DNA, zasady i algorytmy zgodności***

1.1. *Właściwości profili DNA*

Profil DNA może zawierać 24 pary liczb reprezentujących allele 24 loci, które to liczby są także wykorzystywane przez Interpol w procedurach związanych z DNA. Nazwy loci przedstawione są w poniższej tabeli:

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

7 loci na szarym tle w górnym rzędzie stanowią obecny europejski standardowy zestaw loci (ESSOL).

Zasady włączania:

Profile DNA udostępniane przez państwa członkowskie do przeszukania i porównania oraz profile DNA wysyłane do przeszukania i porównania muszą zawierać co najmniej 6 pełnych wyznaczonych loci [1] i mogą zawierać dodatkowe loci lub puste miejsca, zależnie od dostępności loci. Referencyjne profile DNA muszą zawierać co najmniej 6 z 7 loci ESS. W celu zwiększenia trafności zaleca się przechowywanie wszystkich dostępnych alleli w opatrzonej indeksem bazie danych profili DNA.

Profile mieszane są niedozwolone, zatem wartości alleli każdego locus będą składały się tylko z dwóch liczb, które mogą być takie same w przypadku homozygotyczności danego locus.

Symbole wieloznaczne i mikrowarianty należy traktować z zastosowaniem następujących zasad:

— Wszelkie wartości nienumeryczne, z wyjątkiem amelogeniny, zawarte w profilu (np. „o", „f", „r", „na", „nr" lub „un") muszą być automatycznie przekształcone w celu wyeksportowania do symbolu wieloznacznego (*) i przeszukiwane, porównując ze wszystkimi.

— Wartości numeryczne „0", „1" lub „99" zawarte w profilu muszą być automatycznie przekształcone w celu wyeksportowania do symbolu wieloznacznego (*) i przeszukiwane, porównując ze wszystkimi.

— Jeżeli na jeden locus przypadają 3 allele, pierwszy allel zostanie zaakceptowany, a pozostałe 2 allele muszą być automatycznie przekształcone w celu wyeksportowania do symbolu wieloznacznego (*) i przeszukiwane, porównując ze wszystkimi.

— Gdy na allel 1 lub 2 lub obydwa przypadają wartości symbolu wieloznacznego, przeszukane zostaną obydwie wersje wartości numerycznej podanej na dany locus (np. 12, * mogą zgadzać się z 12, 14 lub 9, 12).

— Zgodność mikrowariantów pentanukleotydów (Penta D, Penta E & CD4) zostanie ustalona według następujących formuł:

  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

— Zgodność mikrowariantów tetranukleotydów (pozostałe loci w bazie danych Interpolu to tetranukleotydy) zostanie ustalona według następujących formuł:

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

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

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

[1] „Pełne wyznaczenie" oznacza przypisanie wartości również dla rzadkich alleli.

1.2. *Zasady ustalania zgodności*

Porównanie 2 profili DNA będzie prowadzone na podstawie loci, na które w obydwu profilach DNA przypada para wartości alleli. Między obydwoma profilami DNA musi istnieć zgodność w co najmniej 6 loci (poza amelogeniną).

Pełna zgodność (jakość 1) jest określona jako zgodność występująca wtedy, gdy takie same są wszystkie wartości alleli w porównywanych loci zawartych w żądanych profilach DNA oraz w profilach DNA przedstawianych do porównania. Bliska zgodność jest określana jako zgodność, gdy wartość tylko jednego z porównywanych alleli różni się w dwóch porównywanych profilach DNA (jakość 2, 3 i 4). Bliska zgodność jest akceptowana jedynie wtedy, gdy w dwóch porównywanych profilach DNA znajduje się co najmniej 6 w pełni zgodnych loci.

Przyczyną bliskiej zgodności może być:

— błąd w pisowni popełniony przez człowieka w chwili wpisywania jednego z profili DNA we wniosku o przeszukanie lub w bazie danych DNA,

— błąd w ustalaniu i typowaniu alleli w trakcie procedury generowania profilu DNA.

1.3. *Zasady sprawozdawczości*

Zgłaszane będą zarówno przypadki pełnej, jak i bliskiej zgodności.

Zgłoszenie zgodności będzie przesyłane do krajowego punktu kontaktowego występującego z wnioskiem i zostanie także udostępnione krajowemu punktowi kontaktowemu otrzymującemu wniosek (w celu umożliwienia mu oszacowania charakteru i liczby ewentualnych kolejnych wniosków o dalsze dostępne dane osobowe i inne informacje związane z profilem DNA odpowiadającym trafieniu zgodnie z art. 5 i art. 10 decyzji 2008/615/WSiSW).

2. ***Tabela kodów państw członkowskich***

Zgodnie z decyzją 2008/615/WSiSW kody ISO 3166-1 alfa-2 są wykorzystywane do ustalania nazw domen i innych parametrów konfiguracyjnych wymaganych w programowaniu do wymiany danych DNA przez zamkniętą sieć na mocy decyzji z Prüm.

Kody 3166-1 alfa-2 są to następujące dwuliterowe kody państw członkowskich.

Nazwy państw członkowskich	Kod	Nazwy państw członkowskich	Kod
Belgia	BE	Luksemburg	LU
Bułgaria	BG	Węgry	HU
Republika Czeska	CZ	Malta	MT
Dania	DK	Niderlandy	NL
Niemcy	DE	Austria	AT
Estonia	EE	Polska	PL
Grecja	EL	Portugalia	PT
Hiszpania	ES	Rumunia	RO
Francja	FR	Słowacja	SK
Irlandia	IE	Słowenia	SI
Włochy	IT	Finlandia	FI
Cypr	CY	Szwecja	SE
Łotwa	LV	Zjednoczone Królestwo	UK
Litwa	LT		

3. ***Analiza funkcjonalna***

3.1. *Dostępność systemu*

Wnioski zgodnie z art. 3 decyzji 2008/615/WSiSW powinny docierać do docelowej bazy danych w porządku chronologicznym, natomiast odpowiedzi powinny docierać do państwa członkowskiego, które złożyło wniosek, w ciągu 15 minut od dotarcia wniosku.

3.2. *Drugi krok*

Gdy państwo członkowskie otrzyma zgłoszenie o zgodności, jego krajowy punkt kontaktowy jest odpowiedzialny za porównanie wartości profilu przedłożonego w formie zapytania i wartości profilu (profili) otrzymanych jako odpowiedź w celu zatwierdzenia i sprawdzenia wartości dowodowej profilu. Krajowe punkty kontaktowe mogą się wzajemnie kontaktować do celów zatwierdzenia.

Procedury pomocy prawnej rozpoczynają się po zatwierdzeniu faktycznej zgodności dwóch profili, na podstawie „pełnej zgodności" lub „bliskiej zgodności" uzyskanej w fazie automatycznej konsultacji.

4. ***Dokument kontroli interfejsu DNA***

4.1. *Wstęp*

4.1.1. Cele

Niniejszy rozdział określa wymogi wymiany informacji o profilach DNA między systemami baz danych DNA wszystkich państw członkowskich. Pola nagłówków są określone specjalnie do celów wymiany danych DNA na mocy decyzji z Prüm, część dotycząca danych jest oparta na części schematu XML określonego dla pomostu wymiany danych Interpolu nt. DNA.

Dane wymieniane są z wykorzystaniem protokołu SMTP i innych najnowocześniejszych technologii, wykorzystując centralny serwer poczty udostępniony przez dostawcę sieci. Plik XML jest przesyłany jako treść wiadomości.

4.1.2. Zakres

Dokument ten określa wyłącznie treść wiadomości (pocztowej). Wszystkie tematy odnoszące się do konkretnej sieci i poczty są określane jednolicie w celu umożliwienia zastosowania wspólnej bazy technicznej do wymiany danych DNA.

Obejmuje to:

— format pola tematu w wiadomości w celu umożliwienia zautomatyzowanego przetwarzania wiadomości,

— kwestię konieczności szyfrowania treści, a jeśli tak, to określenie metod, które należy zastosować,

— maksymalną długość wiadomości.

4.1.3. Struktura i zasady formatu XML

Struktura wiadomości XML składa się z następujących części:

— nagłówka zawierającego informacje o przekazie oraz

— części z danymi zawierającej informacje o profilu oraz sam profil.

Ten sam schemat XML zostaje wykorzystany do wniosku i odpowiedzi.

Do celów całościowej weryfikacji niezidentyfikowanych profili DNA (art. 4 decyzji 2008/615/WSiSW) możliwe jest przesłanie partii profili w jednej wiadomości. Należy określić maksymalną liczbę profili w jednej wiadomości. Liczba zależy od maksymalnej dopuszczalnej wielkości wiadomości i określana jest po wyborze serwera poczty.

Przykład XML:

<?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> struktura danych powtórzona, jeżeli wiele profili przesłano (….) w jednej wiadomości SMTP; dozwolone tylko w przypadkach art. 4

</datas>]

</PRUEMDNA>

4.2. *Definicja struktury XML*

Następujące definicje są przeznaczone do celów dokumentacji i lepszej czytelności; prawdziwe, wiążące informacje są przekazane w pliku w schemacie XML (PRUEM DNA.xsd).

4.2.1. Schemat PRUEMDNAx

Zawiera następujące pola:

Pola	Rodzaj	Opis
nagłówek	PRUEM_header	Występuje: 1
dane	PRUEM_datas	Występuje: 1 … 500

4.2.2. Treść struktury nagłówka

4.2.2.1. Nagłówek PRUEM

Poniżej znajduje się struktura opisująca nagłówek pliku XML. Zawiera on następujące pola:

Pola	Rodzaj	Opis
direction	PRUEM_header_dir	Kierunek przepływu wiadomości
ref	String	Oznaczenie pliku XML
generator	String	Generujący plik XML
schema_version	String	Numer wersji schematu do wykorzystania
requesting	PRUEM_header_info	Informacje o państwie członkowskim, które wystąpiło z wnioskiem
requested	PRUEM_header_info	Informacje o państwie członkowskim, do którego zwrócono się z wnioskiem

4.2.2.2. PRUEM_header dir

Rodzaj danych zawartych w wiadomości; wartość może być następująca:

Wartość	Opis
R	Wniosek

Wartość	Opis
A	Odpowiedź

4.2.2.3. Informacje o nagłówku PRUEM

Opis państwa członkowskiego oraz daty/godziny wiadomości. Zawiera następujące pola:

Pola	Rodzaj	Opis
source_isocode	String	Kod ISO 3166-2 państwa członkowskiego, które wystąpiło z wnioskiem
destination_isocode	String	Kod ISO 3166-2 państwa członkowskiego otrzymującego wniosek
request_id	String	Niepowtarzalny identyfikator wniosku
date	Date	Data utworzenia wiadomości
time	Time	Godzina utworzenia wiadomości

4.2.3. Treść danych profilu PRUEM

4.2.3.1. PRUEM_datas

Poniżej znajduje się struktura opisująca część danych XML dotyczącą profilu. Zawiera on następujące pola:

Pola	Rodzaj	Opis
reqtype	PRUEM request type	Rodzaj wniosku (art. 3 lub 4)
date:	Date	Przechowywany profil daty
type	PRUEM_datas_type	Rodzaj profilu
result	PRUEM_datas_result	Wynik wniosku
agency	String	Nazwa odpowiedniej jednostki odpowiedzialnej za profil
profile_ident	String	Niepowtarzalny identyfikator państwa członkowskiego
message	String	Zawiadomienie o błędzie, jeżeli wynik = E
profile	IPSG_DNA_profile	Jeżeli kierunek = A (odpowiedź) ORAZ wynik ≠ H (trafienie) pusty
match_id	String	W przypadku HIT PROFILE_ID (identyfikatora trafionego profilu) profilu będącego przedmiotem wniosku
quality	PRUEM_hitquality_type	Jakość trafienia
hitcount	Integer	Liczba zgodnych alleli
rescount	Integer	Liczba zgodnych profili. Jeżeli kierunek = R (wniosek), to puste. Jeżeli jakość = 0 (pierwotny wnioskowany profil) – puste

4.2.3.2. PRUEM_request_type

Rodzaj danych zawartych w wiadomości; wartość może być następująca:

Wartość	Opis
3	Wnioski zgodne z art. 3 decyzji 2008/615/WSiSW
4	Wnioski zgodne z art. 4 decyzji 2008/615/WSiSW

4.2.3.3. PRUEM_hitquality_type

Wartość	Opis
0	W odniesieniu do profilu z pierwotnego wniosku: „No Hit" („brak trafienia"): wyłącznie odesłanie pierwotnego profilu; „Hit" („trafienie"): odesłanie pierwotnego profilu oraz zgodnych profili
1	Identyczny pod względem wszystkich dostępnych alleli bez symboli wieloznacznych
2	Identyczny pod względem wszystkich dostępnych alleli z symbolami wieloznacznymi
3	Trafienie z odchyleniem (mikrowariant)
4	Trafienie z niedokładną zgodnością

4.2.3.4. PRUEM_data_type

Rodzaj danych zawartych w wiadomości; wartość może być następująca:

Wartość	Opis
P	Profil osoby
S	Wymaz

4.2.2.5. PRUEM_data_result

Rodzaj danych zawartych w wiadomości; wartość może być następująca:

Wartość	Opis
U	Nieokreślony, jeżeli kierunek = R (wniosek)
H	Trafienie
N	Brak trafienia
E	Błąd

4.2.3.6. IPSG_DNA_profile

Struktura opisująca profil DNA. Zawiera następujące pola:

Pola	Rodzaj	Opis
ess_issol	IPSG_DNA_ISSOL	Grupa loci odpowiadająca ISSOL (standardowemu zestawowi loci Interpolu)
additional_loci	IPSG_DNA_additional_loci	Pozostałe loci
marker	String	Metoda generowania DNA
profile_id	String	Niepowtarzalny identyfikator profilu DNA

4.2.3.7. IPSG_DNA_ISSOL

Struktura zawierająca loci z ISSOL (standardowego zestawu loci Interpolu). Zawiera następujące pola:

Pola	Rodzaj	Opis
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Pola	Rodzaj	Opis
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 amelogeniny

4.2.3.8. IPSG_DNA_additional_loci

Struktura zawierająca pozostałe loci. Zawiera następujące pola:

Pola	Rodzaj	Opis
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

Struktura opisująca locus. Zawiera następujące pola:

Pola	Rodzaj	Opis
low_allele	String	Najniższa wartość allela
high_allele	String	Najwyższa wartość allela

5. ***Struktura zastosowania, bezpieczeństwa i komunikacji***

5.1. *Przegląd*

Przy wdrażaniu oprogramowania do wymiany danych DNA w ramach decyzji 2008/615/WSiSW zostanie wykorzystana wspólna sieć łączności, która będzie zamknięta logicznie między państwami członkowskimi. W celu skuteczniejszego wykorzystywania tej wspólnej infrastruktury łączności polegającej na wysyłaniu wniosków i

otrzymywaniu odpowiedzi, przyjmuje się asynchroniczny mechanizm przekazywania wniosków o dane DNA i daktyloskopijne w wiadomości mailowej SMTP. Dla większego bezpieczeństwa będzie wykorzystywany mechanizm sMIME jako przedłużenie funkcji SMTP w celu utworzenia prawdziwego bezpiecznego na całej długości tunelu w sieci.

System operacyjny TESTA (Trans European Services for Telematics between Administrations – transeuropejska sieć telematyczna do wymiany danych między jednostkami administracyjnymi) jest wykorzystywany jako sieć łączności do wymiany danych między państwami członkowskimi. Za system TESTA jest odpowiedzialna Komisja Europejska. Uwzględniając fakt, że krajowe bazy danych DNA oraz obecne krajowe punkty kontaktowe TESTA mogą znajdować się na różnych stronach państw członkowskich, dostęp do systemu TESTA może być utworzony przez:

1) wykorzystywanie obecnego krajowego punktu dostępu lub utworzenie nowego krajowego punktu dostępu do systemu TESTA; lub

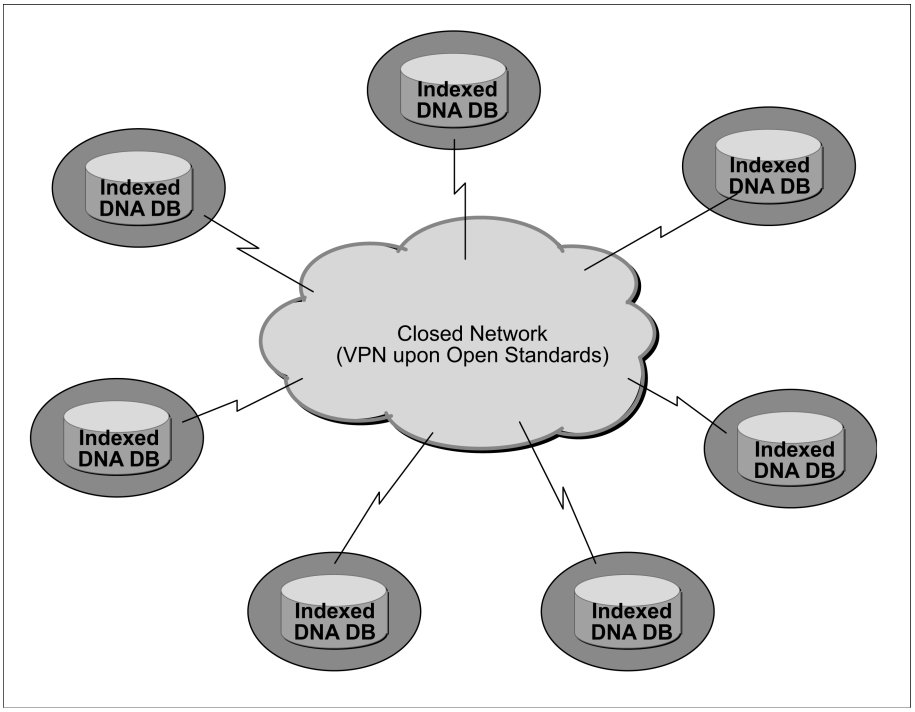
2) utworzenie bezpiecznego miejscowego powiązania ze strony, na której znajduje się baza danych DNA zarządzana przez właściwą agencję krajową, do obecnego punktu dostępu do systemu TESTA.

Protokoły i normy używane przy wprowadzaniu w życie decyzji 2008/615/WSiSW są zgodne z normami otwartymi i spełniają wymogi przedstawiane przez krajowych decydentów z zakresu polityki bezpieczeństwa w państwach członkowskich.

5.2. *Architektura górnego szczebla*

W ramach decyzji 2008/615/WSiSW każde państwo członkowskie będzie udostępniać swoje dane DNA do wymiany z innymi państwami członkowskimi lub przeszukania przez nie zgodnie z standardowym wspólnym formatem danych. Architektura ta oparta jest na modelu łączności „każdy z każdym". Nie istnieje ani centralny serwer komputerowy, ani scentralizowana baza danych zawierająca profile DNA.

Rysunek 1. Topologia wymiany danych DNA



Oprócz spełniania wymogów prawnych dotyczących stron państw członkowskich każde państwo członkowskie może postanowić, jakiego rodzaju sprzętu i oprogramowania należy używać do konfiguracji na jego stronach, tak by spełniać wymogi przedstawione w decyzji 2008/615/WSiSW.

5.3. *Normy bezpieczeństwa i ochrona danych*

Uwzględniono i wdrożono trzy poziomy bezpieczeństwa.

5.3.1. Poziom danych

Dane o profilu DNA przekazane przez każde państwo członkowskie muszą być przygotowane zgodnie ze wspólną normą ochrony danych, tak by państwo członkowskie występujące z wnioskiem otrzymało odpowiedź wskazującą głównie HIT (trafienie) lub NO-HIT (brak trafienia) wraz z numerem identyfikacyjnym w przypadku trafienia, która nie zawiera żadnych informacji osobowych. Dalsze dochodzenie po powiadomieniu o trafieniu będzie prowadzone w sposób dwustronny stosownie do istniejących krajowych przepisów prawa i zasad organizacyjnych obowiązujących na stronach odpowiednich państw członkowskich.

5.3.2. Poziom łączności

Wiadomości zawierające informacje o profilu DNA (wnioski i odpowiedzi) będą szyfrowane z wykorzystaniem wysokiej klasy mechanizmu zgodnego z normami otwartymi, takimi jak sMIME, przed przekazaniem ich na strony państw członkowskich.

5.3.3. Poziom transmisji

Wszystkie zaszyfrowane wiadomości zawierające informacje o profilu DNA będą przekazywane na strony innych państw członkowskich przez wirtualny niepubliczny system tunelowania administrowany na szczeblu międzynarodowym przez zaufanego dostawcę sieci oraz przez zabezpieczone połączenia do tego systemu leżące w gestii danego kraju. Ten wirtualny prywatny system tunelowania nie musi mieć punktu połączenia z powszechną siecią Internetu.

5.4. *Protokoły i normy, które mają być wykorzystywane do szyfrowania: sMIME i pakiety z nim związane*

Do szyfrowania wiadomości zawierających informacje o profilu DNA będzie wykorzystywany otwarty standard sMIME jako rozszerzenie faktycznego standardu SMTP wiadomości mailowych. Protokół sMIME (V3) dopuszcza przekazywanie podpisanych potwierdzeń otrzymania, etykiet bezpieczeństwa i zabezpieczonych list mailingowych i jest nałożony na Cryptographic Message Syntax (CMS), specyfikację IETF dotyczącą wiadomości zabezpieczanych szyfrem. Można go używać do cyfrowego podpisywania, przetwarzania, zatwierdzania lub szyfrowania każdej formy danych cyfrowych.

Bazowy certyfikat wykorzystywany przez mechanizm sMIME musi być zgodny z normą X.509. W celu zapewnienia wykorzystywania norm i procedur wspólnych dla programów Prüm zasady przetwarzania mające zastosowanie do operacji szyfrowania w sMIME lub w ramach różnych środowisk COTS (ogólnodostępne produkty komercyjne) są następujące:

— kolejność operacji: najpierw szyfrowanie, następnie podpis,

— algorytm szyfrowania AES (Advanced Encryption Standard – zaawansowany standard szyfrowania) o długości klucza 256 bitów i RSA o długości klucza 1 024 bitów są stosowane odpowiednio do szyfrowania symetrycznego i asymetrycznego,

— stosuje się algorytm rozpraszający SHA-1.

Funkcja sMIME jest wbudowana w przeważającą większość współczesnych pakietów oprogramowania poczty elektronicznej, takich jak Outlook, Mozilla Mail oraz Netscape Communicator 4.x i działa między wszystkimi głównymi pakietami oprogramowania poczty elektronicznej.

Z racji tego, że sMIME łatwo wprowadza się do krajowych infrastruktur informatycznych na wszystkich stronach państw członkowskich, jest on wybrany jako sprawny mechanizm wprowadzania zabezpieczenia komunikacji. Aby sprawniej osiągnąć cel, jakim jest „Słuszność koncepcji", i obniżyć koszty, do prototypowania wymiany danych DNA wyznaczony jest jednak otwarty standard JavaMail API. Standard ten zakłada proste szyfrowanie i rozszyfrowywanie wiadomości mailowych, wykorzystując sMIME lub OpenPGP. Celem jest tutaj zapewnienie prostego, łatwego w użytkowaniu API dla klientów poczty pragnących wysyłać i otrzymywać szyfrowane wiadomości pocztowe w którymkolwiek z dwóch najpopularniejszych formatów szyfrowania poczty. Tak więc wszelkie wysokiej klasy wdrożenia JavaMail API – takie jak produkt Bouncy Castle JCE (Java Cryptographic Extension – rozszerzenie kryptograficzne Java), który będzie wykorzystany do wdrożenia sMIME do prototypowania wymiany danych DNA między wszystkimi państwami członkowskimi – będą wystarczające do spełnienia wymogów decyzji 2008/615/WSiSW.

5.5. *Architektura aplikacji*

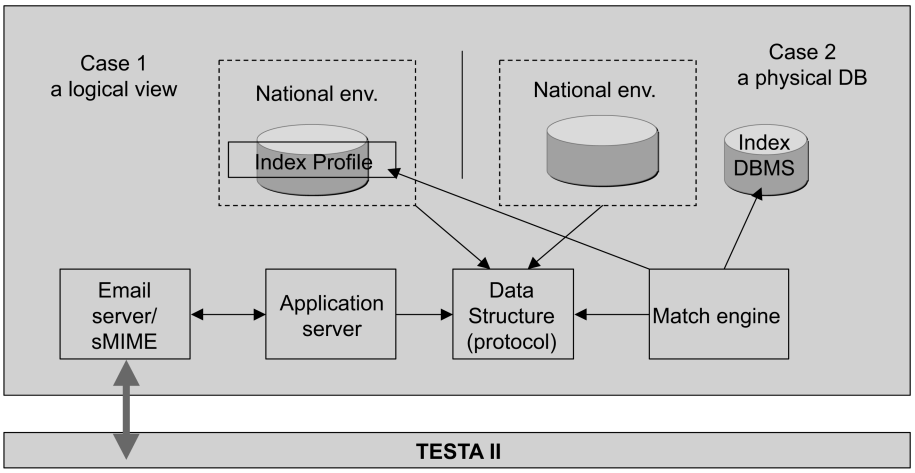
Każde państwo członkowskie udostępni pozostałym państwom członkowskim zestaw standardowych danych profilu DNA zgodnych z obecnym wspólnym ICD. Można tego dokonać przez udostępnienie wglądu do poszczególnych krajowych baz danych lub przez utworzenie fizycznej eksportowanej bazy danych.

Cztery główne komponenty: serwer poczty/sMIME, serwer aplikacji, obszar struktury danych do pozyskiwania/wprowadzania danych i rejestrowania wychodzących/przychodzących wiadomości oraz funkcja ustalania zgodności (Match Engine) wprowadzają całe oprogramowanie w sposób niezależny od danego produktu.

Aby umożliwić wszystkim państwom członkowskim łatwe wprowadzenie tych komponentów na strony krajowe, określona funkcja wspólna została wdrożona za pomocą komponentów otwartych (typu „open source"), które każde państwo członkowskie może wybrać w zależności od jego krajowej polityki informatycznej i przepisów. Z powodu niezależnych elementów, które należy wdrożyć, by mieć dostęp do indeksowanych baz danych zawierających profile DNA objętych decyzją 2008/615/WSiSW, każde państwo członkowskie może swobodnie wybierać podstawowy sprzęt i oprogramowanie, także systemy operacyjne i baz danych.

Opracowano i z powodzeniem przetestowano na obecnej wspólnej sieci prototyp wymiany danych DNA. Wersja 1.0 została wprowadzona do środowiska produkcyjnego i jest używana do codziennych operacji. Państwa członkowskie mogą korzystać ze wspólnie opracowanego produktu, ale mogą także opracować własne produkty. Komponenty wspólnego produktu zostaną utrzymane, indywidualnie dostosowane i dalej rozwinięte zgodnie ze zmieniającymi się wymogami informatyki, medycyny sądowej lub policji.

Rysunek 2. Zarys topologii aplikacji



5.6. *Zasady i normy, które mają być wykorzystywane w strukturze aplikacji*

5.6.1. XML

Wymiana danych DNA będzie korzystała w całości ze schematu XML jako załącznika do wiadomości pocztowych w formacie SMTP. Format XML (Extensible Markup Language) jest zalecanym przez W3C językiem znaczników ogólnego zastosowania służącym do tworzenia języków znaczników szczegółowego zastosowania, mogących służyć do opisywania wielu rodzajów danych. Opis profilu DNA zdatnego do wymiany między wszystkimi państwami członkowskimi został dokonany z wykorzystaniem języka i schematu XML w dokumencie ICD.

5.6.2. Standard dostępu do baz danych ODBC

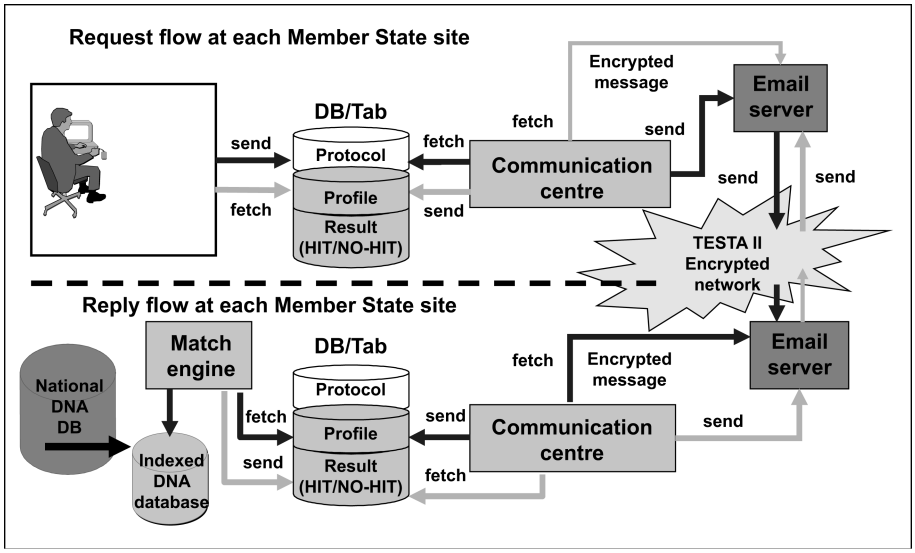
Standard ODBC daje standardową metodę oprogramowania API do uzyskiwania dostępu do systemów zarządzania bazami danych i uniezależnia ją od języków oprogramowania, systemów baz danych i systemów operacyjnych. Standard ODBC ma jednak pewne wady. Administrowanie dużą liczbą urządzeń podległych może pociągać za sobą korzystanie z różnorodnych sterowników i plików DLL. Ta złożoność może zwiększyć koszty administrowania systemem.

5.6.3. Łącze JDBC

Łącze JDBC (Java DataBase Connectivity) jest interfejsem programowania do języka programowania Java określającym sposób, w jaki klient może uzyskać dostęp do bazy danych. W przeciwieństwie do ODBC łącze JDBC nie wymaga korzystania z konkretnego zestawu plików DLL na danym komputerze.

Sposób przetwarzania wniosków o profile DNA i odpowiedzi na nie na stronie każdego państwa członkowskiego jest opisany na poniższym rysunku. Przepływy wniosków i odpowiedzi współdziałają z neutralnym obszarem danych obejmującym różne pule danych mające wspólną strukturę.

Rysunek 3. Zarys działania oprogramowania na stronie każdego państwa członkowskiego



5.7. *Środowisko komunikacyjne*

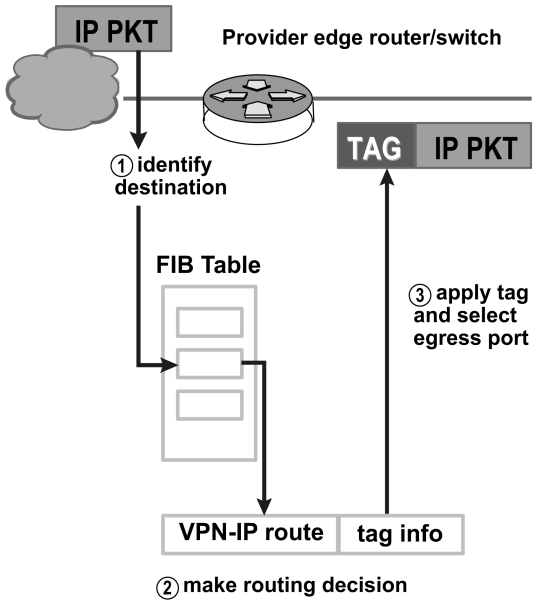
5.7.1. Wspólna sieć komunikacyjna: TESTA i infrastruktura poboczna

Aplikacja wymiany danych DNA będzie wykorzystywała pocztę elektroniczną – mechanizm asynchroniczny – do wysyłania wniosków i otrzymywania odpowiedzi między państwami członkowskimi. Ponieważ wszystkie państwa członkowskie posiadają co najmniej jeden krajowy punkt dostępu do sieci TESTA, wymiana danych DNA będzie prowadzona w tej sieci. TESTA, poprzez swoją funkcję przekazywania poczty, zapewnia liczne dodatkowe usługi. Oprócz utrzymywania skrzynek pocztowych sieci TESTA infrastruktura ta może wprowadzać listy dystrybucyjne poczty elektronicznej i polityki routingu. TESTA może być tym sposobem wykorzystywana jako punkt pośredni dla wiadomości adresowanych do administracji podłączonych do domen w całej UE. Można także wprowadzić oprogramowanie antywirusowe.

Przekaźnik poczty sieci TESTA jest skonstruowany na platformie sprzętowej o dużej dostępności, zlokalizowanej w centralnym obiekcie TESTA i chronionej przez zaporę ogniową. System DNS (Domain Name Services) TESTA będzie przypisywał identyfikatory do adresów IP i ukrywał adresy użytkownika i aplikacji.

5.7.2. Względy bezpieczeństwa

Koncepcja sieci VPN (Virtual Private Network – wirtualna sieć prywatna) została wdrożona w ramach sieci TESTA. Technologia Tag Switching wykorzystywana do skonstruowania sieci VPN będzie ewoluować, tak by wspierać standard technologii MPLS opracowanej przez organizację IETF (Internet Engineering Task Force).



MPLS jest technologią w standardzie IETF, która przyspiesza przepływ komunikacji w sieci przez omijanie analizy pakietowej przez routery pośrednie. Jest to dokonywane na podstawie tzw. etykiet, które dołączane są do pakietów przez końcowe routery połączeń na podstawie informacji przechowywanych w bazie informacji przekazywanych (FIB). Etykiety są także wykorzystywane do wprowadzania wirtualnych sieci prywatnych VPN.

Technologia MPLS łączy w sobie korzyści routingu trójwarstwowego z przełączaniem dwuwarstwowym. Ponieważ adresy IP nie są oceniane podczas przekazywania przez sieć, MPLS nie nakłada żadnych ograniczeń na adresy IP.

Ponadto wiadomości pocztowe przesyłane przez sieć TESTA będą chronione przez mechanizm szyfrujący oparty na standardzie sMIME. Nikt, kto nie zna klucza i nie posiada odpowiedniego certyfikatu, nie może rozszyfrować wiadomości przesyłanych przez sieć.

5.7.3. Protokoły i standardy, które mają być wykorzystywane w sieci łączności

5.7.3.1. SMTP

Protokół SMTP jest faktycznym standardem przesyłania poczty elektronicznej w Internecie. Jest to stosunkowo prosty, oparty na tekście protokół, w ramach którego określony jest co najmniej jeden odbiorca wiadomości, po czym tekst wiadomości jest transmitowany. SMTP korzysta z portu 25 protokołu TCP (Transmission Control Protocol – protokół kontroli transmisji) według specyfikacji IETF. Aby ustalić serwer SMTP dla danej nazwy domeny, wykorzystuje się wymianę poczty (MX) systemu DNS.

Ponieważ protokół ten początkowo był oparty wyłącznie na kodzie ASCII, nie radził sobie dobrze z plikami binarnymi. Standardy takie jak MIME zostały opracowane w celu kodowania plików binarnych do transmisji przez protokół SMTP. Obecnie większość serwerów SMTP rozpoznaje rozwinięcia 8-bitowe MIME i sMIME, umożliwiając przesyłanie plików binarnych prawie tak łatwo jak zwykły tekst. Zasady przetwarzania dla operacji sMIME są opisane w części dotyczącej sMIME (zob. rozdział 5.4).

SMTP jest protokołem typu *push*, który nie pozwala na „wyciąganie" (*pull*) wiadomości ze zdalnego serwera na żądanie. Aby tego dokonać, klient musi korzystać z protokołu POP3 lub IMAP. W ramach wprowadzania wymiany danych DNA postanowiono korzystać z protokołu POP3.

5.7.3.2. Protokół POP

Lokalni użytkownicy poczty elektronicznej używają protokołu pocztowego w wersji 3 (POP3) – standardowego protokołu internetowego z warstwami aplikacji – do ściągania wiadomości pocztowych ze zdalnego serwera za pośrednictwem połączenia TCP/IP. Wykorzystując profil SMTP Submit zawarty w protokole SMTP, użytkownicy poczty przesyłają wiadomości przez Internet lub przez sieć firmową. MIME stanowi standard dla załączników i tekstu w standardzie innym niż ASCII znajdujących się w wiadomościach pocztowych. Wprawdzie ani protokół POP3, ani SMTP nie wymaga poczty elektronicznej sformatowanej w standardzie MIME, jednak ogólnie internetowa poczta elektroniczna jest sformatowana w tym standardzie, zatem użytkownicy protokołu POP muszą także rozumieć standard MIME i z niego korzystać. Ogólna sfera łączności przedstawiona w decyzji 2008/615/WSiSW będzie zatem obejmowała komponenty standardu POP.

5.7.4. Przydzielanie adresu sieciowego

Środowisko operacyjne

Europejski urząd ds. rejestracji adresów IP (RIPE) przydzielił niedawno sieci TESTA specjalny blok podsieci klasy C. W miarę potrzeby dalsze bloki mogą być przydzielone sieci TESTA w przyszłości. Przydzielanie adresów IP państwom członkowskim jest oparte na schemacie geograficznym w Europie. Wymiana danych DNA między państwami członkowskimi w ramach decyzji 2008/615/WSiSW odbywa się w ogólnoeuropejskiej zamkniętej logicznie sieci IP.

Środowisko testowe

Aby zapewnić środowisko umożliwiające niezakłócone codzienne działanie sieci między wszystkimi zainteresowanymi państwami członkowskimi, niezbędne jest utworzenie środowiska testowego w zamkniętej sieci dla nowych państw członkowskich przygotowujących się do przystąpienia do działań w sieci. Określono arkusz parametrów, obejmujący adresy IP, ustawienia sieciowe, domeny poczty elektronicznej oraz konta użytkowników aplikacji i powinien on być wprowadzony na stronie odpowiedniego państwa członkowskiego. Ponadto do celów testowych skonstruowano zestaw profili DNA.

5.7.5. Parametry konfiguracji

Bezpieczny system poczty elektronicznej jest utworzony z wykorzystaniem domeny eu-admin.net. Domena ta, wraz ze związanymi z nią adresami, nie będzie dostępna z lokalizacji poza dostępną w całej UE domeną TESTA, ponieważ nazwy znane są jedynie na centralnym serwerze DNS sieci TESTA, która jest odseparowana od Internetu.

Odwzorowania adresów stron sieci TESTA (nazw hostów) według ich adresów IP dokonuje system DNS sieci TESTA. Dla każdej domeny lokalnej do tego centralnego serwera sieci TESTA zostanie dodany wpis pocztowy, przekazujący wszystkie wiadomości pocztowe przesyłane do domen lokalnych sieci TESTA do centralnego przekaźnika poczty sieci TESTA. Przekaźnik ten będzie następnie przesyłał te wiadomości do konkretnego serwera domeny lokalnej, wykorzystując adres poczty elektronicznej domeny lokalnej. Przy takim sposobie przekazywania poczty niezwykle ważne informacje zawarte w wiadomościach pocztowych będą przechodziły wyłącznie przez ogólnoeuropejską zamkniętą infrastrukturę sieciową, nie zaś przez niezabezpieczony Internet.

Niezbędne jest utworzenie poddomen (oznaczonych ***pogrubioną czcionką i kursywą***) na stronach wszystkich państw członkowskich, o następującej strukturze:

„***application-type*.pruem.*Member State-code***.eu-admin.net", gdzie:

„***Member State-code***" (kod państwa członkowskiego) oznacza dwuliterowy kod danego państwa członkowskiego (tj. AT, BE itd.),

„***application-type***" (rodzaj aplikacji) oznacza jedną z wartości: DNA i FP.

Stosując wyżej wymieniony system, poddomeny dotyczące poszczególnych państw członkowskich są wskazane w poniższej tabeli:

Państwa członkowskie	Poddomena	Komentarze
BE	***dna*.pruem.be**.eu-admin.net	Utworzenie bezpiecznego lokalnego połączenia z aktualnym punktem dostępu do TESTA II
	***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	Wykorzystanie aktualnego krajowego punktu dostępu do TESTA II
	***fp*.pruem.de**.eu-admin.net	
EE	***dna*.pruem.ee**.eu-admin.net	
	***fp*.pruem.ee**.eu-admin.net	

Państwa członkowskie	Poddomena	Komentarze
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	Wykorzystanie aktualnego krajowego punktu dostępu do TESTA II
	***fp*.pruem.es**.eu-admin.net	
FR	***dna*.pruem.fr**.eu-admin.net	Wykorzystanie aktualnego krajowego punktu dostępu do TESTA II
	***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	Wykorzystanie aktualnego krajowego punktu dostępu do TESTA II
	***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	Zamiar stworzenia nowego punktu dostępu do TESTA II w Holenderskim Instytucie Medycyny Sądowej (NFI)
	***fp*.pruem.nl**.eu-admin.net	
AT	***dna*.pruem.at**.eu-admin.net	Wykorzystanie aktualnego krajowego punktu dostępu do TESTA II
	***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	

Państwa członkowskie	Poddomena	Komentarze
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	*Do uzupełnienia:*
	***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	

Rozdział 2: **Wymiana danych daktyloskopijnych (dokument kontroli interfejsu)**

Celem następującego dokumentu kontroli interfejsu jest określenie wymogów wymiany informacji daktyloskopijnych między posiadanymi przez państwa członkowskie systemami automatycznej identyfikacji daktyloskopijnej (AFIS). Dokument ten oparty jest na wdrożonej przez Interpol normie ANSI/NIST-ITL 1-2000 (INT-I, wersja 4.22b).

Wersja ta obejmuje wszystkie podstawowe definicje dla rekordów logicznych typu 1, typu 2, typu 4, typu 9, typu 13 i typu 15 wymaganych do przetwarzania daktyloskopijnego na podstawie obrazów i minucji.

1. ***Zawartość pliku w zarysie***

Plik daktyloskopijny składa się z kilku rekordów logicznych. Istnieje szesnaście rodzajów rekordów określonych w oryginalnym standardzie ANSI/NIST-ITL 1-2000. Między każdym rekordem a polami i subpolami w obrębie rekordów używane są odpowiednie separatory ASCII.

Do wymiany informacji między agencją pierwotną a agencją przeznaczenia wykorzystuje się tylko 6 rodzajów rekordów:

typ 1 → informacje transakcyjne,

typ 3 → alfanumeryczne dane osób/sprawy,

typ 4 → wysokorozdzielcze obrazy daktyloskopijne w skali szarości,

typ 9 → zapis minucji,

typ 13 → zapis obrazu śladu, o zmiennej rozdzielczości,

typ 15 → zapis obrazu linii papilarnych dłoni, o zmiennej rozdzielczości.

1.1. *Typ 1 – nagłówek pliku*

Rekord ten zawiera informacje routingowe oraz informacje określające strukturę pozostałej części pliku. Ten typ rekordu określa także rodzaje transakcji mieszczące się w następujących ogólnych kategoriach:

1.2. *Typ 2 – tekst opisu*

Rekord ten zawiera informacje tekstowe przeznaczone dla agencji wysyłających i odbierających.

1.3. *Typ 4 – wysokorozdzielcze obrazy daktyloskopijne w skali szarości*

Rekord ten jest wykorzystywany do wymiany wysokorozdzielczych (ośmiobitowych) obrazów daktyloskopijnych ustalonych na 500 pikseli na cal. Obrazy daktyloskopijne są kompresowane z zastosowaniem algorytmu kompresji obrazów WSQ w proporcji nie większej niż 15:1. Nie należy stosować innych algorytmów kompresji ani obrazów nieskompresowanych.

1.4. *Typ 9 – zapis minucji*

Rekordy typu 9 są wykorzystywane do wymiany danych dotyczących cech charakterystycznych linii papilarnych lub minucji. Ich celem jest przede wszystkim unikanie dublowania procesów szyfrowania AFIS oraz, częściowo, umożliwienie transmitowania szyfrów AFIS, zawierających mniej danych niż odpowiadające im obrazy.

1.5. *Typ 13 – zapis obrazu śladu, o zmiennej rozdzielczości*

Rekord ten używany jest do wymiany wysokorozdzielczych obrazów śladów palców i dłoni wraz z alfanumeryczną informacją tekstową. Rozdzielczość skanowania obrazów wynosi 500 pikseli na cal przy 256 poziomach szarości. Jeżeli jakość obrazu śladu jest dostateczna, jest on kompresowany z zastosowaniem algorytmu WSQ. W razie konieczności rozdzielczość obrazów można rozszerzyć do wartości ponad 500 pikseli na cal i ponad 256 poziomów szarości w drodze porozumienia dwustronnego. W tym przypadku stanowczo zaleca się używanie JPEG 2000 (zob. dodatek 7).

1.6. *Zapis obrazu dłoni, o zmiennej rozdzielczości*

Zapisy obrazów w oznaczonych polach typu 15 używane są do wymiany obrazów odbitek linii papilarnych dłoni o wysokiej rozdzielczości wraz z alfanumeryczną informacją tekstową. Rozdzielczość skanowania obrazów wynosi 500 pikseli/cal przy 256 poziomach szarości. W celu zminimalizowania ilości danych wszystkie obrazy odbitek dłoni są kompresowane z zastosowaniem algorytmu WSQ. W razie konieczności rozdzielczość obrazów można rozszerzyć do wartości ponad 500 pikseli/cal i ponad 256 poziomów szarości w drodze porozumienia dwustronnego. W tym przypadku stanowczo zaleca się używanie JPEG 2000 (zob. dodatek 7).

2. ***Format rekordu***

Plik transakcji składa się z co najmniej jednego rekordu logicznego. Dla każdego rekordu logicznego zawartego w pliku istnieje kilka pól informacyjnych właściwych dla danego typu rekordu. Każde pole informacyjne może zawierać co najmniej jeden podstawowy element informacji jednowartościowej. Razem elementy te służą przekazywaniu różnych aspektów danych zawartych w tym polu. Pole informacyjne może również składać się z jednego lub więcej elementów informacji zgrupowanych i wielokrotnie powtórzonych w obrębie pola. Taka grupa informacji jest określana jako subpole. Pole informacyjne może zatem składać się z co najmniej jednego subpola zawierającego elementy informacji.

2.1. *Separatory informacji*

W rekordach logicznych oznaczonych pól mechanizmy wydzielające informacje są wprowadzane przez zastosowanie czterech separatorów informacji ASCII. Wydzielonymi informacjami mogą być elementy w polu lub subpolu, pola w obrębie rekordu logicznego lub wielokrotne występowanie subpól. Separatory informacji są określone w standardzie ANSI X3.4. Znaki te są wykorzystywane do rozdzielania i modyfikacji informacji w sensie logicznym. W strukturze hierarchicznej znak separatora pliku „FS" jest najszerszy, po nim następuje separator grupy „GS", separator rekordów „RS" i separator jednostki „US". Tabela 1 zawiera wykaz tych separatorów ASCII oraz opis ich zastosowania w ramach tego standardu.

Separatory informacji należy postrzegać praktycznie jako wskazanie rodzaju danych, które następnie się pojawiają. Znak „US" rozdziela poszczególne elementy informacji w polu lub subpolu. Oznacza to, że następny element informacji to dane do tego pola lub subpola. Wiele subpól w jednym polu, oddzielonych znakiem „RS", oznacza początek następnej grupy powtórzonych elementów informacji. Separator „GS" wstawiony między pola informacji oznacza początek nowego pola poprzedzającego numer identyfikacyjny pola, który się pojawi. Podobnie, początek nowego rekordu logicznego jest oznaczony przez pojawienie się znaku „FS".

Te cztery znaki mają znaczenie jedynie wtedy, gdy są wykorzystywane jako separatory elementów danych w polach rekordów tekstowych ASCII. Występowanie tych znaków w binarnych rekordach obrazów i polach binarnych nie ma konkretnego znaczenia – znaki te są częścią wymienianych danych.

Normalnie nie powinno być pustych pól ani elementów informacji, zatem między dwoma elementami danych powinien widnieć tylko jeden separator. Wyjątek od tej reguły występuje wtedy, gdy dane w polach lub elementy informacji w transakcji są niedostępne, brakuje ich lub są nieobowiązkowe, a przetwarzanie transakcji nie zależy od obecności tych konkretnych danych. W tych przypadkach separatory mnogie i przyległe widnieją razem, nie wymagając wprowadzenia danych fikcyjnych pomiędzy separatory.

Aby określić pole składające się z trzech elementów informacji, stosuje się, co następuje. Jeżeli brakuje informacji do drugiego elementu, dwa przyległe separatory informacji „US" wystąpią między pierwszym i trzecim elementem informacji. Jeżeli brakuje zarówno drugiego, jak i trzeciego elementu informacji, należy stosować trzy separatory – dwa znaki „US" oraz separator kończący pole lub subpole. Ogólnie, jeżeli w polu lub subpolu nie jest dostępny co najmniej jeden obowiązkowy lub nieobowiązkowy element informacji, to należy wprowadzić odpowiednią liczbę separatorów.

Możliwe są kombinacje położonych obok siebie dwóch lub więcej dostępnych separatorów. Gdy dane do elementów informacji, pól lub subpól są niedostępne lub brakuje ich, musi być o jeden separator mniej niż liczba wymaganych elementów danych, subpól lub pól.

Tabela 1. Wykorzystywane separatory

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. *Układ rekordów*

W przypadku rekordów logicznych oznaczonych pól każde wykorzystywane pole informacji jest numerowane zgodnie z tym standardem. Format dla każdego pola składa się z numeru rekordu logicznego, po którym następuje kropka „.", numer pola z dwukropkiem „:", po czym następują informacje właściwe dla tego pola. Numer pola oznaczonego może być numerem składającym się z jednej do dziewięciu cyfr, umieszczonym między kropką „." a dwukropkiem „:". Interpretuje się go jako numer pola o wartości całkowitej. Oznacza to, że numer pola „2123:" jest równy numerowi pola „2.000000123:" i ma być interpretowany w ten sam sposób.

Do celów ilustracji w całym niniejszym dokumencie stosuje się trzycyfrowy numer do numerowania pól zawartych w każdym rekordzie logicznym oznaczonych pól opisanym w tym dokumencie. Numery pól mają formę „TT.xxx:", gdzie „TT" oznacza typ rekordu zaznaczony jednym lub dwoma znakami, po których następuje kropka. Następne trzy znaki oznaczają odpowiedni numer pola, po którym następuje dwukropek. Po dwukropku znajdują się informacje opisowe ASCII lub dane obrazów.

Rekordy logiczne typu 1 i 2 zawierają wyłącznie tekstowe pola danych ASCII. W przypadku każdego z tych dwóch typów cała długość rekordu (łącznie z numerami pól, dwukropkami i separatorami) zostaje zapisana jako pierwsze pole ASCII. Separator kontrolny pliku „FS" ASCII (oznaczający koniec rekordu logicznego lub transakcji) następuje po ostatnim bajcie informacji ASCII i jest włączony do długości rekordu.

W przeciwieństwie do koncepcji pola oznaczonego rekord typu 4 zawiera wyłącznie dane binarne zapisane jako uporządkowane pola binarne o ustalonej długości. Cała długość rekordu jest zapisywana w pierwszym czterobajtowym polu binarnym każdego rekordu. W przypadku tego rekordu binarnego nie zapisuje się numeru rekordu z kropką ani numeru identyfikacyjnego pola z dwukropkiem. Ponadto ponieważ wszystkie długości pól tego rekordu są stałe lub określone, żaden z czterech separatorów („US", „RS", „GS" lub „FS") nie będzie interpretowany inaczej niż jako dane binarne. Do celów rekordu binarnego znak „FS" nie jest używany jako separator ani jako znak kończący transakcję.

3. ***Rekord logiczny typu 1: nagłówek pliku***

Rekord ten opisuje strukturę pliku, rodzaj pliku i inne ważne informacje. Zestaw znaków używany w polach typu 1 zawiera tylko 7-bitowy szyfr ANSI do wymiany informacji.

3.1. *Pola dla rekordu logicznego typu 1*

3.1.1. Pole 1.001: długość rekordu logicznego (Logical Record Length – LEN)

Pole to zawiera całkowite wyliczenie liczby bajtów w całym rekordzie logicznym typu 1. Pole zaczyna się od oznaczenia „1001:", po którym następuje całkowita długość rekordu obejmująca każdy znak w każdym polu oraz separatory informacji.

3.1.2. Pole 1.002: numer wersji (Version Number – VER)

Aby zagwarantować, że użytkownicy wiedzą, która wersja standardu ANSI/NIST jest stosowana, to czterobajtowe pole określa numer wersji standardu wdrażanego przez oprogramowanie lub system tworzący plik. Pierwsze dwa bajty wyszczególniają główny numer referencyjny wersji, a następne dwa – podrzędny numer rewizji. Na przykład, pierwotny standard z roku 1986 byłby uważany za wersję pierwszą i oznaczony numerem „0100", natomiast obecna wersja ANSI/NIST-ITL 1-2000 ma numer „0300".

3.1.3. Pole 1.003: zawartość pliku (File Content – CNT)

Pole to wyszczególnia każdy z rekordów w pliku według typu i porządku, w którym rekordy widnieją w pliku logicznym. Składa się ono z jednego lub więcej subpól, z których każde z kolei zawiera dwa elementy informacji określające jeden rekord logiczny znajdujący się w bieżącym pliku. Subpola są wprowadzane w tej samej kolejności, w jakiej rekordy są zapisywane i transmitowane.

Pierwszy element informacji w pierwszym subpolu jest oznaczony „1", odnosząc się do rekordu typu 1. Następuje po nim drugi element informacji, który zawiera numer pozostałych rekordów znajdujących się w pliku. Numer ten jest także równy liczbie pozostałych subpól pola 1.003.

Każde z pozostałych subpól jest związane z jednym rekordem w pliku, a kolejność subpól odpowiada kolejności rekordów. Każde subpole zawiera dwa elementy informacji. Pierwszy służy określeniu typu rekordu. Drugi jest identyfikatorem rekordu (IDC). Znak „US" jest stosowany do rozdzielenia obu elementów informacji.

3.1.4. Pole 1.004: rodzaj transakcji (Type of Transaction – TOT)

Pole to zawiera trzyliterowy skrót mnemoniczny oznaczający rodzaj transakcji. Kody te mogą różnić się od używanych przez inne wdrożenia standardu ANSI/NIST.

CPS: przeszukanie karta-karta (Criminal Print-to-Print Search). Transakcja ta jest prośbą o przeszukanie obrazów odbitek linii papilarnych zgromadzonych na karcie daktyloskopijnej z kryminalną bazą kart daktyloskopijnych. Odbitki linii papilarnych danej osoby muszą być dołączone w pliku jako obrazy skompresowane z zastosowaniem algorytmu WSQ.

W przypadku braku trafienia zwrócony zostanie następujący rekord logiczny:

— 1 rekord typu 1,

— 1 rekord typu 2.

W przypadku trafienia zwrócony zostanie następujący rekord logiczny:

— 1 rekord typu 1,

— 1 rekord typu 2,

— 1–14 rekordów typu 4.

Rodzaje transakcji CPS są podsumowane w tabeli A.6.1 (dodatek 6).

PMS: przeszukanie karta-ślad (Print-to-Latent Search). Transakcja ta jest prośbą o przeszukanie obrazów odbitek linii papilarnych z karty daktyloskopijnej z kryminalną bazą obrazów niezidentyfikowanych śladów linii papilarnych (śladów NN). Odpowiedź będzie zawierała decyzję Hit/No-Hit (o trafieniu/nietrafieniu) dla przeszukania w AFIS. Jeżeli istnieje wiele niezidentyfikowanych śladów, zostanie zwróconych wiele transakcji SRE, zawierających po jednym śladzie w każdej. Odbitki linii papilarnych danej osoby muszą być dołączone w pliku jako skompresowany obraz WSQ.

W przypadku braku trafienia zwrócone zostaną następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2.

W przypadku trafienia zwrócone zostaną następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2,

— 1 rekord typu 13.

Rodzaje transakcji PMS są podsumowane w tabeli A.6.1 (dodatek 6).

MPS: przeszukanie ślad-karta (Latent-to-Print Search). Transakcja ta jest prośbą o przeszukanie obrazu śladu z kryminalną bazą kart daktyloskopijnych. Informacje o minucjach śladu i jego obraz (skompresowany WSQ) muszą być dołączone do pliku.

W przypadku braku trafienia zwrócone zostaną następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2.

W przypadku trafienia zwrócone zostaną następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2,

— 1 rekord typu 4 lub typu 15.

Rodzaje transakcji MPS są podsumowane w tabeli A.6.4 (dodatek 6).

MMS: przeszukanie ślad-ślad (Latent-to-Latent Search). W tej transakcji plik zawiera obraz śladu, który należy przeszukać z kryminalną bazą obrazów niezidentyfikowanych śladów linii papilarnych (śladów NN) w celu ustalenia powiązań między różnymi miejscami przestępstw. Informacje o minucjach śladu oraz obraz (skompresowany z zastosowaniem WSQ) muszą być zawarte w pliku.

W przypadku braku trafienia zwrócone zostaną następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2.

W przypadku trafienia zwrócone zostaną następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2,

— 1 rekord typu 13.

Rodzaje transakcji MMS są podsumowane w tabeli A.6.4 (dodatek 6).

SRE: ta transakcja jest zwracana przez agencję docelową w odpowiedzi na przekazane zapytania daktyloskopijne. Odpowiedź będzie zawierała decyzję o trafieniu lub braku trafienia wynikającą z przeszukania AFIS w miejscu docelowym. Jeżeli istnieje wiele potencjalnych wyników, zostanie przesłanych wiele transakcji SRE, każda zawierająca jeden wynik (jednego kandydata).

Rodzaje transakcji SRE są podsumowane w tabeli A.6.2 (dodatek 6).

ERR: transakcja ta jest przesyłana przez docelowy system AFIS w celu wskazania błędu transakcji. Zawiera pole wiadomości (ERM) określające wykryty błąd. Zostaną zwrócone następujące rekordy logiczne:

— 1 rekord typu 1,

— 1 rekord typu 2.

Rodzaje transakcji ERR są podsumowane w tabeli A.6.3 (dodatek 6).

Tabela 2. Dopuszczalne kody w transakcjach

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	—	—	—	—

Wyjaśnienie:

M = obowiązkowe
M* = można wprowadzić tylko jeden z obydwu typów rekordów
O = nieobowiązkowe
C = zależne od dostępności danych
— = niedozwolone
1* = zależne od systemów dotychczasowych

3.1.5. Pole 1.005: data transakcji (DAT)

Pole to oznacza datę rozpoczęcia transakcji i musi ono być zgodne z normą zapisywania ISO: YYYYMMDD,

gdzie YYYY oznacza rok, MM – miesiąc, a DD – dzień miesiąca. Przy liczbach jednocyfrowych stosuje się początkowe zera. Na przykład zapis „19931004" oznacza 4 października 1993 r.

3.1.6. Pole 1.006: priorytet (PRY)

To nieobowiązkowe pole określa priorytet wniosku według skali od 1 do 9. „1" jest najwyższym priorytetem, a „9" – najniższym. Transakcje oznaczone priorytetem „1" są przetwarzanie niezwłocznie.

3.1.7. Pole 1.007: identyfikator agencji docelowej (Destination Agency Identifier – DAI)

Pole to wyszczególnia docelową agencję dla danej transakcji.

Składa się ono z dwóch elementów informacji w następującym formacie: CC/*agency* (kod państwa/agencja).

Pierwszy element informacji zawiera kod państwa określony w normie ISO 3166, składający się z dwóch znaków alfanumerycznych. Drugi element – *agency* (agencja) – jest identyfikatorem agencji w wolnym tekście, o maksymalnej długości 32 znaków alfanumerycznych.

3.1.8. Pole 1.008: identyfikator agencji inicjującej (Originating Agency Identifier – ORI)

To pole określa autora pliku i ma ten sam format co DAI (pole 1007).

3.1.9. Pole 1.009: numer kontrolny transakcji (Transaction Control Number – TCN)

Jest to numer kontrolny do celów referencyjnych. Powinien go wygenerować komputer i powinien on mieć następujący format: YYSSSSSSSSA,

gdzie YY oznacza rok transakcji, SSSSSSSS oznacza ośmiocyfrowy numer seryjny, a A jest znakiem kontrolnym tworzonym w wyniku stosowania procedury przedstawionej w dodatku 2.

Gdy TCN nie jest dostępny, pole YYSSSSSSSS zawiera zera oraz znak kontrolny wygenerowany jak wyżej.

3.1.10. Pole 1.010: odpowiedź na transakcję (Transaction Control Response – TCR)

Gdy został wysłany wniosek, na który przysłano odpowiedź, to nieobowiązkowe pole zawiera numer kontrolny transakcji wiadomości wysłanej. Ma ono zatem ten sam format co TCN (pole 1.009).

3.1.11. Pole 1.011: pierwotna rozdzielczość skanowania (Native Scanning Resolution – NSR)

To pole określa normalną rozdzielczość skanowania systemu stosowanego przez inicjatora transakcji. Rozdzielczość jest określana jako dwie cyfry, po których następuje przecinek dziesiętny, a następnie dwie dalsze cyfry.

W odniesieniu do wszystkich transakcji zgodnie z decyzją 2008/615/WSiSW proporcja wynosi 500 pikseli/cal lub 19,68 pikseli/mm.

3.1.12. Pole 1.012: nominalna rozdzielczość transmisji (Nominal Transmitting Resolution – NTR)

To pięciobajtowe pole określa nominalną rozdzielczość transmisji dla transmitowanych obrazów. Rozdzielczość jest wyrażona w pikselach/mm w tym samym formacie jak NSR (pole 1.011).

3.1.13. Pole 1.013: nazwa domeny (Domain Name – DOM)

Obowiązkowe pole określa nazwę domeny dla rekordu logicznego typu 2 z określeniem użytkownika. Składa się ono z dwóch elementów informacji i jest przedstawione jak następuje „INT-I{US}4.22{GS}".

3.1.14. Pole 1.014: czas uniwersalny (GMT)

To obowiązkowe pole przedstawia sposób wyrażania daty i godziny w kategoriach uniwersalnych jednostek czasu uniwersalnego Greenwich (GMT). Pole GMT – gdy jest użytkowane – zawiera uniwersalną datę, oprócz daty lokalnej zawartej w polu 1.005 (DAT). Wykorzystywanie pola GMT eliminuje nieścisłości czasu lokalnego występujące w przypadku gdy transakcja i odpowiedź na nią są przekazywane między dwoma miejscami oddzielonymi kilkoma strefami czasowymi. GMT zapewnia uniwersalne oznaczenie daty i 24-godzinny zegar bez względu na strefy czasowe. Przedstawiany jest jako „CCYYMMDDHHMMSSZ" – sekwencja 15 znaków będąca łańcuchowym połączeniem daty z czasem uniwersalnym Greenwich i kończąca się znakiem „Z". Znaki „CCYY" oznaczają rok transakcji, znaki „MM" oznaczają wartości miesiąca, znaki „DD" oznaczają wartości dnia miesiąca, znaki „HH" oznaczają godzinę, znaki „MM" oznaczają minuty, a znaki „SS" – sekundy. Kompletna data nie przekracza daty bieżącej.

4. ***Rekord logiczny typu 2: tekst opisu***

Struktura większości tego rekordu nie jest określona przez pierwotny standard ANSI/NIST. Rekord zawiera informacje mające konkretne znaczenie dla agencji wysyłających lub otrzymujących plik. W celu dopilnowania, aby komunikujące się systemy daktyloskopijne były zgodne, w rekordzie należy zawrzeć tylko pola wyszczególnione poniżej. Ten dokument określa pola, które są obowiązkowe i nieobowiązkowe, oraz określa strukturę poszczególnych pól.

4.1. *Pola dla rekordu logicznego typu 2*

4.1.1. Pole 2.001: długość rekordu logicznego (Logical Record Length – LEN)

To obowiązkowe pole zawiera długość rekordu typu 2 i określa całkowitą liczbę bajtów, w tym każdy znak w każdym polu w rekordzie oraz separatory informacji.

4.1.2. Pole 2.002: znak oznaczenia obrazu (Image Designation Character – IDC)

Oznaczenie IDC zawarte w tym obowiązkowym polu jest przedstawione w ASCII i określone w polu zawartości pliku (CNT) rekordu typu 1 (pole 1.003).

4.1.3. Pole 2.003: Informacja systemowa (SYS)

Pole to jest obowiązkowe i zawiera cztery bajty oznaczające wersję INT-I, z którą jest zgodny dany rekord typu 2.

Pierwsze dwa bajty określają numer wersji głównej, drugie dwa – drugorzędny numer rewizji. Na przykład obecne oprogramowanie jest oparte na INT-I wersja 4 rewizja 22, zatem jest określone jako „0422".

4.1.4. Pole 2.007: numer sprawy (Case Number – CNO)

Jest to numer, który lokalne biuro daktyloskopijne przyznaje zbiorowi obrazów śladów znalezionych na miejscu przestępstwa. Przyjmuje on następujący format: CC/number (kod państwa/numer),

gdzie CC oznacza kod państwa Interpolu składający się z dwóch znaków alfanumerycznych, a numer jest zgodny z odpowiednimi wytycznymi lokalnymi i może mieć długość do 32 znaków alfanumerycznych.

Pole to umożliwia systemowi rozpoznanie obrazów śladów związanych z konkretnym przestępstwem.

4.1.5. Pole 2.008: numer sekwencji (Sequence Number – SQN)

Pole to określa każdą sekwencję obrazów śladów w danej sprawie. Może ono mieć długość do czterech znaków numerycznych. Sekwencja jest to ślad lub seria śladów zgrupowanych w celu umieszczenia ich w pliku lub przeszukania. Definicja ta oznacza, że nawet pojedynczym śladom należy przypisać numer sekwencji.

Pole to wraz z polem MID (pole 2.009) może być dołączone w celu rozpoznania danego śladu w sekwencji.

4.1.6. Pole 2.009: identyfikator śladów (Latent Identifier – MID)

Pole to określa poszczególny ślad w sekwencji. Przedstawiany jest on jako pojedyncza litera lub dwie litery, przy czym do pierwszego śladu jest przypisana litera A, do drugiego – B i tak dalej do oznaczenia ZZ. To pole wykorzystuje się w sposób analogiczny do numeru sekwencji śladów omówionego w opisie SQN (pole 2.008).

4.1.7. Pole 2.010: numer krajowego rejestru karnego (Criminal Reference Number – CRN)

Jest to niepowtarzalny numer referencyjny przypisany przez krajową agencję osobie po raz pierwszy oskarżonej o popełnienie przestępstwa. W danym kraju żadna osoba nigdy nie posiada więcej niż jeden numer CRN, ten sam numer nie jest także przypisywany więcej niż jednej osobie. Ta sama osoba może jednak mieć numery krajowego rejestru karnego w kilku krajach, które będzie można rozróżnić za pomocą kodu państwa.

Pole CRN posiada następujący format: CC/*number* (kod państwa/numer),

gdzie CC oznacza kod państwa określony w normie ISO 3166 składający się z dwóch znaków alfanumerycznych, a numer jest zgodny z odpowiednimi wytycznymi krajowymi obowiązującymi agencję wydającą i może mieć długość do 32 znaków alfanumerycznych.

W odniesieniu do transakcji zgodnych z decyzją 2008/615/WSiSW to pole będzie wykorzystywane do wprowadzenia krajowego numeru rejestru karnego agencji inicjującej, powiązanego z obrazami w rekordach typu 4 lub typu 15.

4.1.8. Pole 2.012: inny numer identyfikacyjny (MN1)

To pole zawiera numer CRN (pole 2.010) przekazany na drodze transakcji CPS lub PMS bez kodu państwa prowadzącego.

4.1.9. Pole 2.013: inny numer identyfikacyjny (MN2)

To pole zawiera numer CNO (pole 2.007) przekazany na drodze transakcji MPS lub MMS bez kodu państwa prowadzącego.

4.1.10. Pole 2.014: inny numer identyfikacyjny (Miscellaneous Identification Number – MN3)

To pole zawiera numer SQN (pole 2.008) przekazany na drodze transakcji MPS lub MMS.

4.1.11. Pole 2.015: inny numer identyfikacyjny (MN4)

To pole zawiera numer MID (pole 2.009) przekazany na drodze transakcji MPS lub MMS.

4.1.12. Pole 2.063: informacja dodatkowa (Additional Information – INF)

W przypadku transakcji SRE w odpowiedzi na wniosek PMS to pole przekazuje informacje o palcu, którego obraz skutkował ewentualnym trafieniem. Format pola jest, jak następuje:

NN gdzie *NN* oznacza kod pozycji palca określony w tabeli 5, składający się z dwóch cyfr.

We wszystkich pozostałych przypadkach pole to jest nieobowiązkowe. Składa się z maksymalnie 32 znaków alfanumerycznych i może dostarczać dodatkowych informacji o wniosku.

4.1.13. Pole 2.064: wykaz respondentów (Respondents List – RLS)

To pole zawiera co najmniej dwa subpola. Pierwsze subpole opisuje rodzaj przeprowadzonego przeszukania, wykorzystując trzyliterowe skróty mnemoniczne określające rodzaj transakcji w TOT (pole 1.004). Drugie subpole zawiera jeden znak. „I" stosuje się do zaznaczenia trafienia, a „N" stosuje się do zaznaczenia, że nie dokonano trafienia. Trzecie subpole zawiera identyfikator sekwencji potencjalnego wyniku (kandydata) i całkowitą liczbę potencjalnych wyników (kandydatów) oddzieloną ukośnikiem. Jeżeli istnieje wiele potencjalnych trafień, zostanie wysłanych kilka wiadomości.

W przypadku potencjalnego trafienia czwarte subpole będzie zawierało wynik liczący maksymalnie sześć cyfr. Jeżeli trafienie zostało zweryfikowane, wartość tego subpola określa się na „999999".

Przykład: „CPS{RS}I{RS}001/001{RS}999999{GS}".

Jeżeli zdalny system AFIS nie przydziela numerów, to jako odpowiedni punkt należy stosować wartość zero.

4.1.14. Pole 2.074: pole wiadomości o stanie/błędzie (Status/Error Message Field – ERM)

To pole zawiera wiadomości o błędach wynikłych z transakcji, które zostaną odesłane wnioskodawcy w ramach błędnej transakcji.

Tabela 3. Wiadomości informujące o błędach

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.

Wiadomości o błędach w zakresie między 100 a 199:

są one związane z zatwierdzaniem rekordów ANSI/NIST i określane jako:

<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>…

gdzie:

— error_code jest kodem związanym wyłącznie z konkretną przyczyną (zob. tabela 3),

— field_id jest numerem nieprawidłowego pola w standardzie ANSI/NIST (np. 1.001, 2.001, …) w formacie <record_type>.field_id>.sub_field_id>,

— tekst dynamiczny jest bardziej szczegółowym, dynamicznym opisem błędu,

— LF jest to kodowanie końca linii (*Line feed*) oddzielające błędy, jeśli napotkano więcej niż jeden błąd,

— dla rekordów typu 1 ICD jest określony jako „-1".

Przykład:

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

To pole jest obowiązkowe dla transakcji informujących o błędzie.

4.1.15. Pole 2.320: spodziewana liczba kandydatów (Expected Number of Candidates – ENC)

To pole zawiera maksymalną liczbę kandydatów (potencjalnych trafień) do weryfikacji oczekiwanych przez agencję inicjującą. Wartość ENC nie może przekraczać wartości określonych w tabeli 11.

5. ***Rekord logiczny typu 4: obraz o wysokiej rozdzielczości w skali szarości***

Należy odnotować, że rekordy logiczne typu 4 mają charakter binarny, nie zaś według ASCII. Każde pole ma zatem konkretne miejsce przypisane mu w rekordzie, co oznacza, że wszystkie pola są obowiązkowe.

Standard dopuszcza określenie w rekordzie zarówno wielkości obrazu, jak i jego rozdzielczości. Wymaga, aby rekordy logiczne typu 4 zawierały dane obrazów daktyloskopijnych, które są przekazywane z nominalną gęstością pikseli wynoszącą 500–520 pikseli/cal. Gęstość preferowana dla nowych obrazów wynosi 500 pikseli/cal lub 19,68 pikseli/mm. System INT-I określa gęstość 500 pikseli/cal, ale podobne systemy mogą komunikować się ze sobą, stosując gęstość inną niż preferowana w granicach 500–520 pikseli/cal.

5.1. *Pola dla rekordu logicznego typu 4*

5.1.1. Pole 4.001: długość rekordu logicznego (LEN)

To czterobajtowe pole zawiera długość rekordu typu 4 i określa całkowitą liczbę bajtów, w tym każdy bajt w każdym polu w rekordzie.

5.1.2. Pole 2.002: oznaczenie obrazu (IDC)

Jest to jednobajtowe binarne określenie numeru IDC podanego w pliku głównym.

5.1.3. Pole 4.003: rodzaj obrazu (IMP)

Jest to jednobajtowe pole umiejscowione na szóstym bajcie rekordu.

Tabela 4. Rodzaj obrazu palca

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. Pole 4.004: pozycja palca (Finger Position – FGP)

To 6-bajtowe pole o stałej długości jest umiejscowione od siódmej do dwunastej pozycji bajtu rekordu typu 4. Zawiera ono ewentualne pozycje palców, zaczynając od bajtu z lewej strony (bajt 7 rekordu). Znana lub najbardziej prawdopodobna pozycja palca jest pobierana z tabeli 5. Można umieścić odniesienia do maksymalnie pięciu dodatkowych palców, wprowadzając alternatywne pozycje palców w pozostałych pięciu bajtach, wykorzystując ten sam format. Jeżeli ma być wykorzystanych mniej niż pięć odniesień do pozycji palców, niewykorzystane bajty należy wypełnić binarnym 255. W celu wskazania wszystkich pozycji palców stosuje się kod 0 oznaczający pozycję nieznaną.

Tabela 5. Kod pozycji palców i maksymalna wielkość

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

Do śladów na miejscu przestępstwa należy stosować tylko kody od 0 do 10.

5.1.5. Pole 4.005: rozdzielczość skanowania obrazu (Image Scanning Resolution – ISR)

To jednobajtowe pole znajduje się na 13. bajcie rekordu typu 4. Jeżeli zawiera symbol „0”, to obraz został pobrany w preferowanej rozdzielczości 19,68 pikseli/mm (500 pikseli/cal). Jeżeli zawiera ono symbol „1”, oznacza to, że obraz został pobrany w innej rozdzielczości określonej w rekordzie typu 1.

5.1.6. Pole 4.006: długość linii poziomej (Horizontal Line Length – HLL)

To pole jest umiejscowione w bajtach 14 i 15 w rekordzie typu 4. Określa ono liczbę pikseli zawartych w każdej linii skanu. Najbardziej znaczący będzie pierwszy bajt.

5.1.7. Pole 4.007: długość linii pionowej (Vertical Line Length – VLL)

To pole zawiera, w bajtach 16 i 17, liczbę linii skanowania w obrazie. Najbardziej znaczący jest pierwszy bajt.

5.1.8. Pole 4.008: algorytm kompresji obrazu w skali szarości (Gray-scale Compression Algorithm – GCA)

To jednobajtowe pole określa algorytm kompresji w skali szarości stosowany do kodowania danych obrazu. Do tego wdrożenia kod binarny 1 oznacza, że wykorzystano program kompresji WSQ (dodatek 7).

5.1.9. Pole 4.009: obraz

To pole zawiera strumień bajtów reprezentujący obraz. Jego struktura będzie naturalnie zależna od zastosowanego algorytmu kompresji.

6. ***Rekord logiczny typu 9: zapis minucji***

Rekordy typu 9 zawierają tekst w kodzie ASCII opisujący minucje i związane z nimi informacje pochodzące od śladu. Do celów transakcji przeszukania obrazów śladów nie ma ograniczeń dla liczby rekordów typu 9 w pliku; każdy rekord dotyczy innego obrazu lub śladu.

6.1. *Wyciąg minucji*

6.1.1. Identyfikacja rodzaju minucji

Ta norma określa trzy numery identyfikatora stosowane do opisania rodzaju minucji. Są one przedstawione w tabeli 6. Zakończenie linii papilarnej jest oznaczone jako typ 1. Rozwidlenie jest oznaczone jako typ 2. Jeżeli dana minucja nie może być wyraźnie skategoryzowana jako jeden z wyżej wymienionych typów, jest oznaczana jako „inna" – typ 0.

Tabela 6. Rodzaje minucji

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Umiejscowienie i rodzaj minucji

Aby szablony odpowiadały sekcji 5 normy ANSI INCITS 378-2004, do ustalania umiejscowienia (lokalizacji i kierunku kąta) poszczególnych minucji będzie stosowana następująca metoda, ulepszająca obecną normę INCITS 378-2004.

Pozycją lub lokalizacją minucji przedstawiającej koniec linii papilarnej jest punkt rozwidlenia grzbietu bruzdy bezpośrednio przed zakończeniem linii papilarnej. Jeżeli trzy odnogi bruzdy zostały zredukowane do struktury o szerokości jednego piksela, punkt przecięcia jest lokalizacją minucji. Podobnie lokalizacją minucji rozwidlenia jest punkt rozwidlania grzbietu linii papilarnej. Jeżeli każda z trzech odnóg linii została zredukowana do szerokości jednego piksela, punkt przecięcia trzech odnóg jest lokalizacją minucji.

Po przekształceniu wszystkich końców linii papilarnych w rozwidlenia wszystkie minucje obrazu daktyloskopijnego są przedstawiane jako rozwidlenia. Współrzędne pikseli X i Y przecięcia trzech odnóg każdej minucji mogą być formatowane bezpośrednio. Ustalenie kierunku minucji może być dokonane na podstawie każdego rozwidlenia grzbietu. Należy zbadać trzy odnogi każdego rozwidlenia grzbietu i ustalić punkt zakończenia każdej odnogi. Rysunek 6.1.2 ilustruje trzy metody stosowane do ustalenia punktu zakończenia odnogi, które są oparte na rozdzielczości skanowania 500 pikseli/cal.

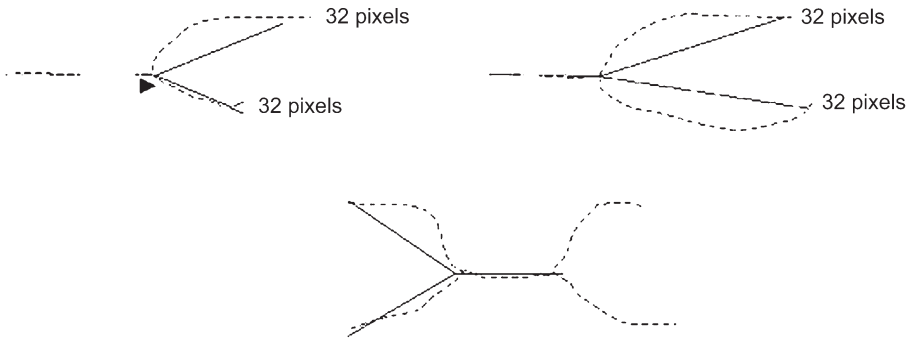
Zakończenie ustala się według zdarzenia, które występuje najpierw. Wyliczenie pikseli jest oparte na rozdzielczości skanowania wynoszącej 500 pikseli/cal. Różne rozdzielczości oznaczają różne wyliczenia pikseli.

— Odległość wynosząca .064" (32. piksel),

— koniec odnogi grzbietu występujący między odległością .02" a .064" (od 10. do 32. piksela); krótsze odnogi nie są wykorzystywane,

— drugie rozwidlenie występuje w obrębie odległości .064" (przed 32. pikselem).

Rysunek 6.1.2.



Kąt minucji jest ustalany przez utworzenie trzech wirtualnych promieni rozpoczynających się w punkcie rozwidlenia i sięgających do końca każdej odnogi. Najmniejszy z trzech kątów utworzonych przez promienie jest przecięty w celu wyznaczenia kierunku minucji.

6.1.3. Układ współrzędnych

Układ współrzędnych stosowany do wyrażenia minucji obrazu odbitki linii papilarnych palca jest układem kartezjańskim. Lokalizacje minucji są przedstawiane przez współrzędne x i y. Początkiem systemu współrzędnych jest górny lewy róg pierwotnego obrazu, przy czym wartości x zwiększają się w kierunku prawej strony, a wartości y – w dół. Współrzędne x i y danej minucji są przedstawiane w jednostkach pikseli od początku. Należy odnotować, że umiejscowienie początku i jednostek miary nie jest zgodne z normą stosowaną przy określaniu rekordów typu 9 w ramach ANSI/NIST-ITL 1-2000.

6.1.4. Kierunek minucji

Kąty są wyrażane w standardowym formacie matematycznym – zero stopni po prawej stronie i zwiększające się kąty w kierunku przeciwnym do wskazówek zegara. Zapisane kąty wskazują kierunek wsteczny wzdłuż linii papilarnej do jej końca, a przy rozwidleniu – w stronę środka bruzdy. Jest to przeciwne o 180 stopni wobec normy kątów określonej w definicji typu 9 w normie ANSI/NIST-ITL 1-2000.

6.2. *Pola do rekordu logicznego typu 9 w formacie INCITS-378*

Wszystkie pola rekordów typu 9 są zapisywane jako tekst w formacie ASCII. W tym rekordzie o oznaczonym polu nie są dopuszczalne pola binarne.

6.2.1. Pole 9.001: długość rekordu logicznego (LEN)

To obowiązkowe pole w formacie ASCII zawiera długość rekordu i określa całkowitą liczbę bajtów, w tym każdy znak w każdym polu w rekordzie.

6.2.2. Pole 9.002: oznaczenie obrazu (IDC)

To obowiązkowe dwubajtowe pole jest stosowane do identyfikacji i lokalizacji danych minucji. IDC zawarte w tym polu jest zgodne z IDC znajdującym się w polu zawartości pliku rekordu typu 1.

6.2.3. Pole 9.003: rodzaj obrazu (IMP)

To obowiązkowe jednobajtowe pole opisuje sposób uzyskania informacji o obrazie daktyloskopijnym. W celu oznaczenia rodzaju obrazu do pola zostaje wprowadzona wartość ASCII właściwego kodu wybranego z tabeli 4.

6.2.4. Pole 9.004: format minucji (Minutiae Format – FMT)

To pole zawiera symbol „U" oznaczające, że minucje są sformatowane w kategoriach M1-378. Nawet jeżeli informacje są kodowane zgodnie z normą M1-378, wszystkie pola danych w rekordzie typu 9 muszą pozostać w formie pól tekstowych ASCII.

6.2.5. Pole 9.126: informacje o CBEFF (Common Biometric Exchange File Format – wspólnym formacie pliku wymiany danych biometrycznych)

To pole zawiera trzy elementy informacji. Pierwszy z nich zawiera wartość „27" (0x1B). Jest to identyfikacja posiadacza formatu CBEFF przyznana przez Międzynarodowe Stowarzyszenie Branży Biometrycznej (IBIA) komitetowi technicznemu INCITS M1. Znak <US> oddziela ten element od typu formatu CBEFF mającego wartość „513" (0x0201) oznaczającą, że ten rekord zawiera tylko dane o miejscu i kierunku kąta bez informacji

dotyczących rozszerzonego bloku danych. Znak <US> oddziela ten element od identyfikatora produktu CBEFF określającego „posiadacza" sprzętu kodującego. Tę wartość ustala sprzedający. Można ją uzyskać na stronie internetowej IBIA (www.ibia.org), jeżeli jest tam podana.

6.2.6. Pole 9.127: rozpoznanie sprzętu do pozyskiwania

To pole zawiera dwa elementy informacji oddzielone znakiem <US>. Pierwszy zawiera „APPF", jeżeli sprzęt pierwotnie wykorzystany do pozyskania obrazu miał zaświadczenie o zgodności z dodatkiem F (Specyfikacja jakości obrazu IAFIS, 29 stycznia 1999 r.) do dok. CJIS-RS-0010 – specyfikacji elektronicznej transmisji obrazów palców FBI. Jeżeli sprzęt nie był zgodny ze wspomnianą specyfikacją, pole będzie zawierało oznaczenie „NONE". Drugi element informacji zawiera identyfikator sprzętu do pozyskiwania, który jest numerem produktu przyznawanym przez jego sprzedawcę. Wartość „0" oznacza, że identyfikator sprzętu nie jest wyszczególniony.

6.2.7. Pole 9.128: długość linii poziomej (Horizontal Line Length – HLL)

Obowiązkowe pole ASCII zawiera liczbę pikseli mieszczących się na pojedynczej poziomej linii przekazywanego obrazu. Maksymalna wielkość pozioma jest ograniczona do 65 534 pikseli.

6.2.8. Pole 9.129: długość linii pionowej (Vertical Line Length – VLL)

Obowiązkowe pole ASCII zawiera liczbę linii poziomych w przekazywanym obrazie. Maksymalna wielkość pionowa jest ograniczona do 65 534 pikseli.

6.2.9. Pole 9.130: jednostki skali (Scale Units – SLC)

To obowiązkowe pole ASCII określa jednostki używane do opisania częstotliwości pobierania obrazu (gęstości pikseli). „1" w tym polu oznacza ilość pikseli na cal, a „2" oznacza ilość pikseli na centymetr. „0" w tym polu oznacza brak podanej skali. W tym wypadku iloraz HPS/VPS daje proporcję pikseli.

6.2.10. Pole 9.131: skala pikseli poziomych (Horizontal Pixel Scale – HPS)

To obowiązkowe pole ACII określa wyrażoną w liczbach całkowitych gęstość pikseli w kierunku poziomym, o ile pole SLC zawiera symbol „1" lub „2". W innych przypadkach oznacza ono poziomy komponent proporcji pikseli.

6.2.11. Pole 9.132: skala pikseli pionowych (Vertical Pixel Scale – VPS)

To obowiązkowe pole ACII określa wyrażoną w liczbach całkowitych gęstość pikseli w kierunku pionowym, o ile pole SLC zawiera symbol „1" lub „2". W innych przypadkach oznacza ono pionowy komponent proporcji pikseli.

6.2.12. Pole 9.133: widok palca

To obowiązkowe pole zawiera numer palca związanego z danymi w tym rekordzie. Numer zaczyna się od 0 i zwiększa się o 1 do 15.

6.2.13. Pole 9.134: pozycja palca (Finger Position – FGP)

To pole zawiera kod oznaczający pozycję palca, która wygenerowała informacje w tym rekordzie typu 9. Kod zawierający cyfry od 1 do 10 znajdujący się w tabeli 5 lub odpowiedni kod dłoni z tabeli 10 jest stosowany do oznaczania pozycji palca lub dłoni.

6.2.14. Pole 9.135: jakość palca

To pole zawiera informacje o jakości ogólnych danych o minucjach palca i oznaczone jest cyframi od 0 do 100. Liczba ta jest ogólnym oznaczeniem jakości zapisu palca i oznacza jakość pierwotnego obrazu, ekstrakcji minucji i wszelkie działania dodatkowe mające ewentualny wpływ na zapis minucji.

6.2.15. Pole 9.136: liczba minucji

To obowiązkowe pole zawiera liczbę minucji zapisanych w tym rekordzie logicznym.

6.2.16. Pole 9.137: dane o minucjach palca

To obowiązkowe pole zawiera sześć elementów informacji oddzielonych znakiem <US>. Składa się ono z kilku subpól, z których każde zawiera dane pojedynczej minucji. Całkowita liczba subpól minucji musi zgadzać się z liczbą znajdującą się w polu 136. Pierwszy element informacji to numer indeksu minucji, zaczynający się od „1" i zwiększający się o „1" dla każdej kolejnej minucji w odbitce palca. Drugi i trzeci element informacji to współrzędna x i y minucji wyrażona w jednostkach pikseli. Czwarty element informacji to kąt minucji zapisany w jednostkach dwóch stopni. Wartość ta jest nieujemna i wynosi od 0 do 179. Piąty element informacji to rodzaj minucji. Wartość „0" reprezentuje minucje typu „OTHER" (INNE), „1" – koniec linii papilarnej, a „2" – rozwidlenie. Szósty element informacji oznacza jakość każdej minucji. Wartość ta rozciąga się od 1 jako minimum do 100 jako maksimum. Wartość 0 oznacza brak dostępnego oznaczenia jakości. Każde subpole jest oddzielone od następnego separatorem <RS>.

6.2.17. Pole 9.138: informacje o liczbie linii papilarnych

To pole składa się z serii subpól, z których każde zawiera trzy elementy informacji. Pierwszy element informacji w pierwszym subpolu oznacza metodę wyliczania liczby linii papilarnych. Wartość „0" oznacza, że nie dokonuje się założeń co do metody stosowanej do wyliczania linii papilarnych ani ich kolejności w rekordzie. Wartość „1" oznacza, że dla każdej minucji środkowej dane o liczbie linii zostały uzyskane z dokładnością do najbliższej przyległej minucji w czterech kwadrantach, a wyliczenia linii dla każdej minucji są przedstawione razem. Wartość „2" oznacza, że dla każdej minucji środkowej dane o liczbie linii zostały uzyskane z dokładnością do najbliższej przyległej minucji w ośmiu oktantach, a wyliczenia linii dla każdej minucji są przedstawione razem. Pozostałe dwa elementy informacji w pierwszym subpolu zawierają „0". Elementy informacji są rozdzielone separatorem <US>. Kolejne subpola będą zawierać numer indeksu minucji środkowych jako pierwszy element informacji, numer indeksu przyległych minucji jako drugi element informacji oraz liczbę przeciętych linii jako trzeci element. Subpola są rozdzielone separatorem <RS>.

6.2.18. Pole 9.139: informacje podstawowe

To pole będzie się składało z jednego subpola na każdą informację podstawową obecną w pierwotnym obrazie. Każde subpole składa się z trzech elementów informacji. Pierwsze dwa elementy zawierają współrzędne x i y w jednostkach pikseli. Trzeci element informacji zawiera kąt zapisany w jednostkach 2 stopni. Wartość jest nieujemna i wynosi od 0 do 179. Informacje mnogie są rozdzielone separatorem <RS>.

6.2.19. Pole 9.140: informacje o delcie

To pole będzie się składało z jednego subpola na każdą informację o delcie obecną w pierwotnym obrazie. Każde subpole składa się z trzech elementów informacji. Pierwsze dwa elementy zawierają współrzędne x i y w jednostkach pikseli. Trzeci element informacji zawiera kąt zapisany w jednostkach 2 stopni. Wartość jest nie negatywna i wynosi od 0 do 179. Informacje mnogie są rozdzielone separatorem <RS>.

7. ***Rekord typu 13: obraz śladu, o zmiennej rozdzielczości***

Rekord logiczny typu 13 o oznaczonym polu zawiera dane obrazu pozyskane z obrazów śladów. Obrazy te mają być przekazane agencjom, które automatycznie pozyskają lub spowodują interwencję osób i przetwarzanie w celu pozyskania z obrazów informacji o żądanych cechach.

Informacje dotyczące zastosowanej rozdzielczości skanowania, wielkości obrazu i innych parametrów wymaganych do przetworzenia obrazu są zapisane w rekordzie jako oznaczone pola.

Tabela 7. Wygląd rekordu typu 13: obraz śladu, o zmiennej rozdzielczości

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	—

Klucz do znaków: N = numeryczne; A = alfabetyczne; AN = alfanumeryczne; B = binarne.

7.1. *Pola dla rekordu logicznego typu 13*

Następujące akapity opisują dane zawarte w każdym polu rekordu logicznego typu 13.

W rekordzie logicznym typu 13 wpisy znajdują się w numerowanych polach. Wymagane jest, by pierwsze dwa pola w rekordzie były uporządkowane, a pole zawierające dane obrazu było ostatnim fizycznym polem w rekordzie. Dla każdego pola rekordu typu 13 w tabeli 7 wyszczególniono „kod warunkowy" jako „M" – obowiązkowy i „O" – nieobowiązkowy, numer pola, rodzaj znaków, wielkość pola i granice występowania. W oparciu o trzycyfrowy numer pola w ostatniej kolumnie podane jest wyliczenie maksymalnej liczby bajtów dla danego pola. Ponieważ do wyrażenia numeru pola stosuje się więcej cyfr, maksymalne wyliczenie bajtów także się zwiększy. Dwa wpisy w rubryce „rozmiar pola w każdym przypadku występowania" (*field size per occurrence*) obejmują wszystkie separatory zastosowane w danym polu. „Maksymalna liczba bajtów" (*maximum byte count*) obejmuje numer pola, informacje i separatory, w tym znak „GS".

7.1.1. Pole 13.001: długość rekordu logicznego (LEN)

To obowiązkowe pole ASCII zawiera całkowite wyliczenie liczby bajtów w rekordzie logicznym typu 13. Pole 13.001 określa długość rekordu, w tym każdy znak każdego pola znajdującego się w rekordzie oraz separatory informacji.

7.1.2. Pole 13.002: oznaczenie obrazu (IDC)

To obowiązkowe pole ACII jest wykorzystywane do rozpoznania danych obrazu śladu zawartych w rekordzie. IDC jest zgodny z IDC znajdującym się w polu zawartości pliku (CNT) rekordu typu 1.

7.1.3. Pole 13.003: rodzaj obrazu (IMP)

To obowiązkowe jedno- lub dwubajtowe pole ASCII oznacza sposób uzyskania informacji o obrazie śladu. W polu tym wprowadza się odpowiedni kod śladów wybrany z tabeli 4 (palce) lub tabeli 9 (dłonie).

7.1.4. Pole 13.004: agencja inicjująca/ORI (SRC)

To obowiązkowe pole ASCII zawiera identyfikację administracji lub organizacji, która pierwotnie pozyskała obraz twarzy znajdujący się w rekordzie. Normalnie identyfikator agencji inicjującej (ORI) agencji, która pozyskała obraz będzie zawarty w tym polu. Składa się ono z dwóch elementów informacji w następującym formacie: CC/*agency* (kod państwa/agencja).

Pierwszy element informacji zawiera kod państwa określony przez Interpol składający się z dwóch znaków alfanumerycznych. Drugi element – *agency* (agencja) – jest identyfikatorem agencji w wolnym tekście, o maksymalnej długości 32 znaków alfanumerycznych.

7.1.5. Pole 13.005: data pozyskania obrazu śladu (Latent Capture Date – LCD)

To obowiązkowe pole ASCII zawiera datę pozyskania obrazu śladu zawartego w rekordzie. Data widnieje jako osiem cyfr w formacie CCYYMMDD. Znaki CCYY oznaczają rok pozyskania obrazu; znaki MM oznaczają miesiąc; znaki DD oznaczają dzień miesiąca. Na przykład 20000229 oznacza 29 lutego 2000 r. Kompletna data musi być właściwą datą.

7.1.6. Pole 13.006: długość linii poziomej (HLL)

To obowiązkowe pole ASCII zawiera liczbę pikseli znajdujących się na pojedynczej linii poziomej transmitowanego obrazu.

7.1.7. Pole 13.007: długość linii pionowej (VLL)

To obowiązkowe pole ASCII zawiera liczbę linii poziomych transmitowanego obrazu.

7.1.8. Pole 13.008: jednostki skali (SLC)

To obowiązkowe pole ASCII określa jednostki używane do opisania rozdzielczości obrazu (gęstości pikseli). „1” w tym polu oznacza ilość pikseli na cal, a „2” oznacza ilość pikseli na centymetr. „0” w tym polu oznacza brak podanej skali. W tym wypadku iloraz HPS/VPS daje proporcję pikseli.

7.1.9. Pole 13.009: skala pikseli poziomych (HPS)

To obowiązkowe pole ACII określa wyrażoną w liczbach całkowitych gęstość pikseli w kierunku poziomym, o ile pole SLC zawiera symbol „1” lub „2”. W innych przypadkach oznacza ono poziomy komponent proporcji pikseli.

7.1.10. Pole 13.010: skala pikseli pionowych (VPS)

To obowiązkowe pole ACII określa wyrażoną w liczbach całkowitych gęstość pikseli w kierunku pionowym, o ile pole SLC zawiera symbol „1” lub „2”. W innych przypadkach oznacza ono pionowy komponent proporcji pikseli.

7.1.11. Pole 13.011: algorytm kompresji (Compression Algorithm – CGA)

To obowiązkowe pole ASCII określa algorytm stosowany do kompresji obrazów w skali szarości. Zob. dodatek 7, w którym znajdują się kody kompresji.

7.1.12. Pole 13.012: ilość bitów na piksel (Bits per Pixel – BPX)

To obowiązkowe pole ASCII zawiera liczbę bitów wykorzystanych do przedstawienia jednego piksela. To pole zawiera wpis „8” dla normalnych wartości w skali szarości wynoszących od 0 do 255. Wszelkie wpisy większe niż „8” w tym polu reprezentują piksel w skali szarości z większą precyzją.

7.1.13. Pole 13.013: pozycja palca/dłoni (FGP)

To obowiązkowe oznaczone pole zawiera co najmniej jedną możliwą pozycję palca lub dłoni, która może być zgodna z obrazem śladu. Numer kodu dziesiętnego odpowiadający znanej lub najbardziej prawdopodobnej pozycji palca jest pobrany z tabeli 5 lub odpowiadający najbardziej prawdopodobnej pozycji dłoni – z tabeli 10 i wprowadzony jako subpole ASCII z jednym lub dwoma znakami. Dodatkowe pozycje palców lub dłoni mogą być zaznaczone przez wprowadzenie alternatywnych kodów pozycji jako subpól oddzielonych separatorem „RS”. Kod „0” oznaczający „nieznany palec” stosuje się do zaznaczenia każdej pozycji palca od jednego do dziesięciu. Kod „20” oznaczający „nieznaną dłoń” stosuje się do zaznaczenia każdej wymienionej pozycji dłoni.

7.1.14. Pola 13.014–019: zachowane do określenia w przyszłości (Reserved for Future Definition – RSV)

Te pola są zarezerwowane, by można było w przyszłości wprowadzić zmiany tej normy. Na obecnym poziomie nie należy wykorzystywać żadnego z tych pól. Jeżeli którekolwiek z nich są obecne, należy je ignorować.

7.1.15. Pole 13.020: uwaga (Comment – COM)

To nieobowiązkowe pole można wykorzystać do wprowadzania uwag lub innych informacji tekstowych w kodzie ASCII wraz z danymi obrazu śladu.

7.1.16. Pola 13.021–199: zachowane do określenia w przyszłości (RSV)

Te pola są zarezerwowane, by można było w przyszłości wprowadzić zmiany tej normy. Na obecnym poziomie nie należy wykorzystywać żadnego z tych pól. Jeżeli którekolwiek z nich są obecne, należy je ignorować.

7.1.17. Pola 13.200–998: pola określone przez użytkownika (User-Defined Fields – UDF)

Pola te są możliwe do określenia przez użytkownika i będą używane do przyszłych wymagań. Ich wielkość i zawartość są określane przez użytkownika i są zgodne z agencją otrzymującą. Jeżeli występują, zawierają informacje tekstowe w kodzie ASCII.

7.1.18. Pole 13.999: dane obrazu (Image Data – DAT)

To pole zawiera wszystkie dane z pozyskanego obrazu śladu. Zawsze ma numer pola 999 i musi być ostatnim polem fizycznym w rekordzie. Na przykład po „13.999:" następują dane obrazu w reprezentacji binarnej.

Każdy piksel nieskompresowanych danych w skali szarości jest zwykle przypisany ośmiu bitom (256 poziomów szarości) zawartym w jednym bajcie. Jeżeli wpis w polu BPX 13.012 jest większy lub mniejszy niż 8, to liczba bajtów wymaganych do zawarcia piksela będzie inna. Jeżeli stosuje się kompresję, dane pikseli są skompresowane zgodnie z techniką określoną w polu GCA.

7.2. *Koniec rekordu typu 13: obraz śladu, o zmiennej rozdzielczości*

Do celów spójności separator „FS" jest stosowany bezpośrednio po ostatnim bajcie danych z pola 13.999 w celu oddzielenia go od ostatniego rekordu logicznego. Separator ten musi być włączony w pole długości rekordu typu 13.

8. ***Rekord typu 15: obraz odbitki dłoni, o zmiennej rozdzielczości***

Rekord logiczny o oznaczonym polu typu 15 zawiera dane obrazu odbitki linii papilarnych dłoni i służy do ich wymiany, a także stałe i określone przez użytkownika informacje tekstowe mające znaczenie dla cyfrowego obrazu. Informacje o zastosowanej rozdzielczości skanu, wielkości obrazu i inne parametry lub uwagi wymagane do przetworzenia obrazu są zapisane jako oznaczone pola w rekordzie. Obrazy odbitek linii papilarnych dłoni przekazane innym agencjom będą przetwarzane przez agencje otrzymujące w celu uzyskania pożądanych informacji potrzebnych do stwierdzenia zgodności.

Dane obrazów są pozyskiwane bezpośrednio od danej osoby z zastosowaniem urządzenia skanującego na żywo, lub z karty daktyloskopijnej zawierającej odbitki dłoni lub innych nośników zawierających obrazy odbitek dłoni danej osoby.

Wszelkie metody stosowane do pozyskania obrazów odbitek dłoni są zdolne do pozyskania zestawu obrazów dla każdej ręki. Zestaw ten obejmuje dłoń jako jeden zeskanowany obraz oraz całą dłoń od nadgarstka do końców palców jako jeden lub dwa zeskanowane obrazy. Jeżeli do przedstawienia całej dłoni wykorzystane są dwa obrazy, to dolny obraz obejmuje dłoń od nadgarstka do górnej części między palcami (trzeciego stawu palca) i obszaru kłębu kciuka i poniżej. Górny obraz rozciąga się od części między palcami do końców palców. Umożliwia to odpowiednie nałożenie na siebie części obrazu na obszarze dłoni między palcami. Uzgadniając strukturę linii papilarnych i szczegółów znajdujących się w tej wspólnej części, analityk może stwierdzić, że obydwa obrazy pochodzą od tej samej dłoni.

Ponieważ transakcja obrazu dłoni może być wykorzystana do różnych celów, może ona zawierać różne obszary obrazów pobranych z dłoni lub ręki. Kompletny zestaw obrazów dłoni jednej osoby zwykle zawiera jego dłoń i obraz(-y) całej dłoni obydwu rąk. Jako że rekord logiczny o oznaczonym polu może zawierać tylko jedno pole binarne, jeden rekord typu 15 będzie potrzebny dla każdej dłoni i jeden lub dwa takie rekordy dla każdego obrazu całej dłoni. Zatem cztery do sześciu rekordów typu 15 będzie potrzebnych do przedstawienia obrazów odbitek dłoni danej osoby w normalnej transakcji obrazów dłoni.

8.1. *Pola dla rekordu logicznego typu 15*

Następujące akapity opisują dane zawarte w każdym polu rekordu logicznego typu 15.

W rekordzie logicznym typu 15 wpisy znajdują się w numerowanych polach. Wymagane jest, by pierwsze dwa pola w rekordzie były uporządkowane, a pole zawierające dane obrazu było ostatnim fizycznym polem w rekordzie. Dla każdego pola rekordu typu 15 w tabeli 8 wyszczególniono „kod warunkowy" jako „M" – obowiązkowy i „O" – nieobowiązkowy, numer pola, rodzaj znaków, wielkość pola i granice występowania. W oparciu o trzycyfrowy numer pola, w ostatniej kolumnie podane jest wyliczenie maksymalnej liczby bajtów dla danego pola. Ponieważ do wyrażenia numeru pola stosuje się więcej cyfr, maksymalne wyliczenie bajtów także się zwiększy. Dwa wpisy w rubryce „rozmiar pola w każdym przypadku występowania" (*field size per occurrence*) obejmują wszystkie separatory zastosowane w danym polu. „Maksymalna liczba bajtów" (*maximum byte count*) obejmuje numer pola, informacje i separatory, w tym znak „GS".

8.1.1. Pole 15.001: długość rekordu logicznego (LEN)

To obowiązkowe pole ASCII zawiera całkowite wyliczenie liczby bajtów w rekordzie logicznym typu 15. Pole 15.001 określa długość rekordu, w tym każdy znak każdego pola znajdującego się w rekordzie oraz separatory informacji.

8.1.2. Pole 15.002: oznaczenie obrazu (IDC)

To obowiązkowe pole ACII jest wykorzystywane do rozpoznania obrazu odbitki dłoni zawartych w rekordzie. IDC jest zgodny z IDC znajdującym się w polu zawartości pliku (CNT) rekordu typu 1.

8.1.3. Pole 15.003: rodzaj obrazu (IMP)

To obowiązkowe jednobajtowe pole ASCII oznacza sposób pozyskania informacji o obrazie odbitki dłoni. W tym polu wprowadza się odpowiedni kod wybrany z tabeli 9.

8.1.4. Pole 15.004: agencja inicjująca/ORI (SRC)

To obowiązkowe pole ASCII zawiera identyfikację administracji lub organizacji, która pierwotnie pozyskała obraz znajdujący się w rekordzie. Normalnie identyfikator agencji inicjującej (ORI), która pozyskała obraz będzie zawarty w tym polu. Składa się ono z dwóch elementów informacji w następującym formacie: CC/*agency* (kod państwa/agencja).

Pierwszy element informacji zawiera kod państwa określony przez Interpol składający się z dwóch znaków alfanumerycznych. Drugi element – *agency* (agencja) – jest identyfikatorem agencji w wolnym tekście, o maksymalnej długości 32 znaków alfanumerycznych.

8.1.5. Pole 15.005: data pozyskania obrazu dłoni (Palmprint Capture Date – PCD)

To obowiązkowe pole ASCII zawiera datę pozyskania obrazu odbitki dłoni. Data widnieje jako osiem cyfr w formacie CCYYMMDD. Znaki CCYY oznaczają rok pozyskania obrazu; znaki MM oznaczają miesiąc; znaki DD oznaczają dzień miesiąca. Na przykład 20000229 oznacza 29 lutego 2000 r. Kompletna data musi być właściwą datą.

8.1.6. Pole 15.006: długość linii poziomej (HLL)

To obowiązkowe pole ASCII zawiera liczbę pikseli znajdujących się na pojedynczej linii poziomej transmitowanego obrazu.

8.1.7. Pole 15.007: długość linii pionowej (VLL)

To obowiązkowe pole ASCII zawiera liczbę linii poziomych transmitowanego obrazu.

8.1.8. Pole 15.008: jednostki skali (SLC)

To obowiązkowe pole ASCII określa jednostki używane do opisania rozdzielczości obrazu (gęstości pikseli). „1" w tym polu oznacza ilość pikseli na cal, a „2" oznacza ilość pikseli na centymetr. „0" w tym polu oznacza brak podanej skali. W tym wypadku iloraz HPS/VPS daje proporcję pikseli.

8.1.9. Pole 15.009: skala pikseli poziomych (HPS)

To obowiązkowe pole ASCII określa wyrażoną w liczbach całkowitych gęstość pikseli w kierunku poziomym, o ile pole SLC zawiera symbol „1" lub „2". W innych przypadkach oznacza ono poziomy komponent proporcji pikseli.

8.1.10. Pole 15.010: skala pikseli pionowych (VPS)

To obowiązkowe pole ASCII określa wyrażoną w liczbach całkowitych gęstość pikseli w kierunku pionowym, o ile pole SLC zawiera symbol „1" lub „2". W innych przypadkach oznacza ono pionowy komponent proporcji pikseli.

Tabela 8. Rekord obrazu odbitki dłoni o zmiennej rozdzielczości typu 15

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	—

Tabela 9. Rodzaj obrazu dłoni

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. Pole 15.011: algorytm kompresji (CGA)

To obowiązkowe pole ASCII określa algorytm stosowany do kompresji obrazów w skali szarości. Wpis „NONE" (brak) w tym polu oznacza, że dane zawarte w tym rekordzie są nieskompresowane. W przypadku obrazów, które mają być skompresowane, to pole zawiera preferowaną metodę kompresji obrazów odbitek palców zawartych na karcie daktyloskopijnej. Odnośne kody kompresji są określone w dodatku 7.

8.1.12. Pole 15.012: ilość bitów na piksel (BPX)

To obowiązkowe pole ASCII zawiera liczbę bitów wykorzystanych do przedstawienia jednego piksela. To pole zawiera wpis „8" dla normalnych wartości w skali szarości wynoszących od 0 do 255. Wszelkie wpisy większe lub mniejsze niż „8" w tym polu reprezentują piksel w skali szarości z większą precyzją.

Tabela 10. Kody, obszary i rozmiary dłoni

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. Pole 15.013: pozycja obrazu dłoni (Palmprint Position – PLP)

To obowiązkowe oznaczone pole zawiera pozycję obrazu dłoni odpowiadającą obrazowi odbitki. Kod dziesiętny odpowiadający znanej lub najbardziej prawdopodobnej pozycji obrazu dłoni jest pobierany z tabeli 10 i wprowadzany jako dwuznakowe subpole ASCII. Tabela 10 także wyszczególnia maksymalne obszary obrazu i wymiary dla każdej możliwej pozycji obrazu dłoni.

8.1.14. Pola 15.014–019: zachowane do określenia w przyszłości (RSV)

Te pola są zarezerwowane, by można było w przyszłości wprowadzić zmiany tej normy. Na obecnym poziomie nie należy wykorzystywać żadnego z tych pól. Jeżeli którekolwiek z nich są obecne, należy je ignorować.

8.1.15. Pole 15.020: uwaga (COM)

To nieobowiązkowe pole można wykorzystać do wprowadzania uwag lub innych informacji tekstowych w kodzie ASCII wraz z danymi obrazu odbitki dłoni.

8.1.16. Pola 15.021–199: zachowane do określenia w przyszłości (RSV)

Te pola są zarezerwowane, by można było w przyszłości wprowadzić zmiany tej normy. Na obecnym poziomie nie należy wykorzystywać żadnego z tych pól. Jeżeli którekolwiek z nich są obecne, należy je ignorować.

8.1.17. Pola 15.200–998: pola określone przez użytkownika (UDF)

Pola te są możliwe do określenia przez użytkownika i będą używane do przyszłych wymagań. Ich wielkość i zawartość są określane przez użytkownika i są zgodne z agencją otrzymującą. Jeżeli występują, zawierają informacje tekstowe w kodzie ASCII.

8.1.18. Pole 15.999: dane obrazu (DAT)

To pole zawiera wszystkie dane z pozyskanego obrazu śladu. Zawsze ma numer pola 999 i musi być ostatnim polem fizycznym w rekordzie. Na przykład po „15.999:" następują dane obrazu w reprezentacji binarnej. Każdy piksel nieskompresowanych danych w skali szarości zwykle jest wyrażany jako osiem bitów (256 poziomów szarości) zawartych w jednym bajcie. Jeżeli wpis w polu BPX 15.012 jest większy lub mniejszy niż 8, liczba bajtów potrzebnych do zawarcia piksela będzie się różnić. Jeżeli zastosowano kompresję, to dane pikseli są skompresowane zgodnie z techniką określoną w polu CGA.

8.2. *Koniec rekordu typu 15: obraz odbitki dłoni, o zmiennej rozdzielczości*

Do celów spójności separator „FS" jest stosowany bezpośrednio po ostatnim bajcie danych z pola 15.999 w celu oddzielenia go od ostatniego rekordu logicznego. Separator ten musi być włączony w pole długości rekordu typu 15.

8.3. *Dodatkowe rekordy typu 15: obraz odbitki dłoni, o zmiennej rozdzielczości*

W tym pliku można zawrzeć dodatkowe rekordy typu 15. Dla każdego dodatkowego obrazu odbitki dłoni wymagany jest kompletny rekord logiczny typu 15 wraz z separatorem „FS".

Tabela 11. Maksymalna liczba pozycji przyjętych do weryfikacji od transmisji

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

Rodzaje przeszukań:

TP/TP: karta daktyloskopijna – karta daktyloskopijna,

LT/TP: ślad palca – karta daktyloskopijna,

LP/PP: ślad dłoni – dłoń,

TP/UL: karta daktyloskopijna – ślad NN palca,

LT/UL: ślad palca – ślad NN palca,

PP/ULP: dłoń – ślad NN dłoni,

LP/ULP: ślad dłoni – ślad NN dłoni.

9. ***Dodatki do rozdziału 2 (wymiana danych daktyloskopijnych)***

9.1. *Dodatek 1 Kody rozdzielające ASCII*

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]) Pozycja określona w normie ASCII.

9.2. *Dodatek 2 Obliczanie znaków alfa-numerycznych*

Dla TCN i TCR (pola 1.09 i 1.10):

Liczba odpowiadająca znakowi jest generowana z zastosowaniem następującego wzoru:

(YY * 10^8 + SSSSSSSS) Modulo 23

Gdzie YY i SSSSSSSS są wartościami numerycznymi, odpowiednio, ostatnich dwóch cyfr roku i numeru seryjnego.

Znak kontrolny jest wtedy generowany z tabeli podanej poniżej.

Dla CRO (pole 2.010):

Liczba odpowiadająca znakowi jest generowana z zastosowaniem następującego wzoru:

(YY * 10^6 + NNNNNN) Modulo 23

Gdzie YY i NNNNNN są wartościami numerycznymi, odpowiednio, ostatnich dwóch cyfr roku i numeru seryjnego.

Znak kontrolny jest wtedy generowany z tabeli podanej poniżej.

Tabela znaków kontrolnych

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. *Dodatek 3 Kody znaków*

7-bitowy kod ANSI do wymiany informacji

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	”	#	USD	%	&	’
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	T
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. *Dodatek 4 Podsumowanie transakcji*

Rekord typu 1 (obowiązkowy)

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

W kolumnie „Stan”:

O = nieobowiązkowy; M = obowiązkowy; C = warunkowy, jeżeli transakcja jest odpowiedzią dla agencji inicjującej.

Rekord typu 2 (obowiązkowy)

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	—	—

W kolumnie „Stan”:

O = nieobowiązkowy; M = obowiązkowy; C = warunkowy, jeżeli dane są dostępne,

*) = jeżeli transmisja danych jest zgodna z prawem krajowym (nieobjęta decyzją 2008/615/WSiSW).

9.5. *Dodatek 5 Definicje rekordów typu 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

W kolumnie „Stan": O = nieobowiązkowy; M = obowiązkowy; C = warunkowy.

W kolumnie „Rodzaj znaku" (Character Type): A = alfa; N = numeryczny; B = binarny.

1* dopuszczalne znaki dla nazwy agencji to [„0..9", „A..Z", „a..z", „_", „.", „", „–"]

9.6. *Dodatek 6 Definicje rekordów typu 2*

Tabela A.6.1. Transakcje CPS i 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}

Tabela A.6.2. Transakcje 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	2015: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}

Tabela A.6.3. Transakcje 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 1009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2003 INVALID SYSTEM INFORMATION {GS}

Tabela A.6.4. Transakcje MPS i MMS

Identifie	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}
.	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

O = nieobowiązkowy; M = obowiązkowy; C = warunkowy.

W kolumnie „Rodzaj znaku" (Character Type): A = alfa; N = numeryczny; B = binarny.

1* dopuszczalne znaki to [„0..9", „A..Z", „a..z", „_", „.", „", „–"]

9.7. *Dodatek 7 kody kompresji skali szarości*

Kody kompresji

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 > 500dpi.
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. *Dodatek 8 Specyfikacja poczty*

W celu polepszenia obiegu wewnętrznego temat wiadomości pocztowej transakcji PRUEM musi być wypełniony kodem państwa członkowskiego (CC), które wysłało wiadomość i rodzajem transakcji (TOT pole 1.004).

Format: Kod państwa/rodzaj transakcji

Przykład: „DE/CPS"

Główna część wiadomości może być pusta.

Rozdział 3: **Wymiana danych rejestracyjnych pojazdów**

1. ***Wspólny zestaw danych do zautomatyzowanego przeszukania danych rejestracyjnych pojazdów***

1.1. *Definicje*

Definicje obowiązkowych i nieobowiązkowych elementów danych przedstawione w art. 16 ust. 4 są następujące:

Obowiązkowe (M – Mandatory)

Element danych musi być przekazany, gdy informacje są dostępne w rejestrze krajowym danego państwa członkowskiego. Istnieje zatem obowiązek wymiany informacji, gdy są one dostępne.

Nieobowiązkowe (O – Optional)

Element danych może być przekazany, gdy informacje są dostępne w rejestrze krajowym danego państwa członkowskiego. Nie ma zatem obowiązku wymiany informacji, nawet gdy są one dostępne.

Każdy element w zestawie danych, który jest wyraźnie uznany za ważny w związku z decyzją 2008/615/WSiSW, jest opatrzony oznaczeniem (Y).

1.2. *Wyszukiwanie pojazdu/jego właściciela/posiadacza*

1.2.1. Warunki wyszukiwania

Istnieją dwa sposoby poszukiwania informacji określonej w następnym akapicie:

— według numeru podwozia VIN, daty i godziny odniesienia (nieobowiązkowe),

— według numeru rejestracyjnego, numeru podwozia (nieobowiązkowy), daty i godziny odniesienia (nieobowiązkowe).

Za pomocą tych kryteriów wyszukiwania zostaną przekazane informacje związane z jednym lub niekiedy większą liczbą pojazdów. Jeżeli muszą być przekazane informacje dotyczące tylko jednego pojazdu, wszystkie pozycje są przesyłane w jednej odpowiedzi. Jeżeli zostanie odnaleziona większa liczba pojazdów, państwo członkowskie, do którego się zwrócono, może samo ustalić, które informacje przekazać – wszystkie, czy tylko jedną pozycję w celu zawężenia poszukiwania (np. z przyczyn prywatności lub wydajności działania).

Pozycje niezbędne do zawężenia poszukiwań są przedstawione w pkt 1.2.2.1. W pkt 1.2.2.2 opisane są informacje w całości.

Gdy poszukiwanie odbywa się według numeru podwozia, daty i godziny odniesienia, można je przeprowadzić w jednym państwie członkowskim lub we wszystkich.

Gdy poszukiwanie odbywa się według numeru rejestracyjnego, daty i godziny odniesienia, musi ono być przeprowadzone w jednym konkretnym państwie członkowskim.

Normalnie do poszukiwania wykorzystuje się aktualną datę i godzinę, jest jednak możliwe przeprowadzanie poszukiwania, wykorzystując datę i godzinę odniesienia z przeszłości. Gdy poszukiwanie jest przeprowadzane z wykorzystaniem daty i godziny odniesienia z przeszłości, a informacje historyczne nie są dostępne w rejestrze konkretnego państwa członkowskiego, ponieważ takie informacje nie są w ogóle zarejestrowane, faktyczne informacje mogą być zwrócone z zaznaczeniem, że są to faktyczne informacje.

1.2.2. Zestaw danych

1.2.2.1. Pozycje, które należy przekazać i które są niezbędne do zawężenia poszukiwania

Pozycja	M/O [1]	Uwagi	Prüm Y/N [2]
Dane pojazdu			
Numer rejestracyjny	M		Y
Numer nadwozia/podwozia/ramy VIN	M		Y
Kraj rejestracji	M		Y
Marka	M	(D.1 [3]) np. Ford, Opel, Renault itd.	Y
Nazwa handlowa pojazdu	M	(D.3) np. Focus, Astra, Megane	Y

Pozycja	M/O (1)	Uwagi	Prüm Y/N (2)
Kod kategorii UE	M	(J) motorynki, motorowery, samochody itd.	Y

(1) M = obowiązkowo, jeśli znajduje się w krajowym rejestrze, O = nieobowiązkowo.
(2) Wszystkie atrybuty przypisane indywidualnie przez państwa członkowskie oznaczono symbolem Y.
(3) Zharmonizowany skrót dokumentu, zob. dyrektywa Rady 1999/37/WE z dnia 29 kwietnia 1999 r.

1.2.2.2. Kompletny zestaw danych

Pozycja	M/O (1)	Uwagi	Prüm Y/N
Dane związane z posiadaczem pojazdu		(C.1 (2) dane związane z posiadaczem świadectwa rejestracji	
Nazwisko (firma) posiadacza dowodu rejestracyjnego	M	(C.1.1.) osobne pola na nazwisko, tytuły itd. oraz podane zostanie nazwisko w formacie do wydruku	Y
Imię	M	(C.1.2) osobne pola na imię (imiona) i inicjały oraz podane zostanie nazwisko w formacie do wydruku	Y
Adres	M	(C.1.3) osobne pola na ulicę, numer domu i aneks, kod pocztowy, miejsce pobytu, kraj pobytu itd. oraz zostanie podany adres w formacie do wydruku	Y
Płeć	M	Mężczyzna, kobieta	Y
Data urodzenia	M		Y
Forma prawna	M	Osoba fizyczna, stowarzyszenie, spółka, firma itd.	Y
Miejsce urodzenia	O		Y
Numer identyfikacyjny	O	Identyfikator, który w sposób unikalny identyfikuje osobę lub firmę	N
Rodzaj i numer dokumentu tożsamości	O	Rodzaj i numer dokumentu tożsamości (np. nr paszportu).	N
Data nabycia prawa własności pojazdu	O	Data nabycia prawa własności pojazdu. Data będzie zwykle pokrywać się z datą wydrukowaną pod (I) na dokumencie rejestracyjnym pojazdu.	N
Data do kiedy był posiadaczem pojazdu	O	Data do kiedy był posiadaczem pojazdu.	N
Rodzaj posiadacza	O	Jeśli brak posiadacza pojazdu (C.2), odniesienie do faktu, że posiadacz dokumentu rejestracyjnego: — jest właścicielem pojazdu, — nie jest właścicielem pojazdu, — nie jest określony w dokumencie rejestracyjnym jako właściciel pojazdu.	N
Dane związane z właścicielami pojazdu		(C.2)	
Nazwisko (firma) właścicieli	M	(C.2.1)	Y
Imię	M	(C.2.2)	Y

Pozycja	M/O [1]	Uwagi	Prüm Y/N
Adres	M	(C.2.3)	Y
Płeć	M	Mężczyzna, kobieta	Y
Data urodzenia	M		Y
Forma prawna	M	Osoba fizyczna, stowarzyszenie, spółka, firma itd.	Y
Miejsce urodzenia	O		Y
Numer identyfikacyjny	O	Identyfikuje jednoznacznie osobę lub firmę	N
Rodzaj i numer dokumentu tożsamości	O	Rodzaj i numer dokumentu tożsamości (np. nr paszportu)	N
Data rozpoczęcia posiadania pojazdu	O	Data rozpoczęcia posiadania pojazdu	N
Data zakończenia posiadania pojazdu	O	Data zakończenia posiadania pojazdu	N
Dane pojazdów			
Numer rejestracyjny	M		Y
Numer nadwozia, podwozia, ramy, VIN	M		Y
Kraj rejestracji	M		Y
Marka	M	(D.1) np. Ford, Opel, Renault itd.	Y
Nazwa handlowa pojazdu	M	(D.3) np. Focus, Astra, Megane	Y
Rodzaj pojazdu/kod kategorii UE	M	(J) motorynki, motorowery, samochody itd.	Y
Data pierwszej rejestracji	M	(B) Data pierwszej rejestracji gdziekolwiek na świecie	Y
Data początkowa aktualnej rejestracji	M	(I) Data rejestarcji, do której odwołuje się konkretny dokument rejestracyjny pojazdu	Y
Data końcowa rejestracji	M	Data końcowa rejestarcji, do której odwołuje się konkretny dokument rejestracyjny pojazdu. Możliwe, że ta data oznacza okres ważności tak jak wydrukowano na dokumencie, jeśli nie jest on nieograniczony (skrót na dokumencie = H).	Y
Status	M	Zezłomowany, skradziony, wywieziony z kraju itd.	Y
Data początkowa statusu	M		Y
Data końcowa statusu	O		N
kW	O	(P.2)	Y
Pojemność	O	(P.1)	Y
Rodzaj tablicy rejestracyjnej	O	Stała, tymczasowa itd.	Y
Dokument identyfikacyjny pojazdu 1	O	Numer identyfikacyjny pierwszego dokumentu identyfikacyjnego wydrukowany na dokumencie pojazdu	Y
Dokument identyfikacyjny pojazdu 2 [3]	O	Drugi nr identyfikacyjny pierwszego dokumentu identyfikacyjnego wydrukowany na dokumencie pojazdu	Y
Dane związane z ubezpieczeniem			
Nazwa towarzystwa ubezpieczeniowego	O		Y
Data rozpoczęcia ubezpieczenia	O		Y
Data zakończenia ubezpieczenia	O		Y
Adres	O		Y
Numer ubezpieczenia	O		Y

Pozycja	M/O [1]	Uwagi	Prüm Y/N
Numer identyfikacyjny	O	Identyfikator, który w sposób jednoznaczny identyfikuje firmę	N
Rodzaj nr identyfikacyjnego	O	Rodzaj nru identyfikacyjnego (np. numer izby przemysłowo-handlowej)	N

[1] M = obowiązkowo, jeśli znajduje się w krajowym rejestrze, O = nieobowiązkowo.
[2] Zharmonizowany skrót dokumentu, zob. dyrektywa Rady 1999/37/WE z dnia 29 kwietnia 1999 r.
[3] W Luksemburgu używa się dwóch oddzielnych nrów identyfikacyjnych dokumentu rejestracyjnego rejestracji pojazdu.

2. ***Bezpieczeństwo danych***

2.1. *Przegląd*

Oprogramowanie EUCARIS służy do prowadzenia bezpiecznej łączności między państwami członkowskimi i przekazuje informacje do dotychczasowych systemów państw członkowskich z wykorzystaniem protokołu XML. Państwa członkowskie wymieniają wiadomości przez wysyłanie ich bezpośrednio do odbiorcy. Ośrodek danych danego państwa członkowskiego jest podłączony do sieci TESTA w UE.

Wiadomości XML przesyłane przez sieć są szyfrowane. Technika szyfrowania wiadomości to SSL. Wiadomości wysyłane do terminala końcowego mają postać zwykłego tekstu XML, ponieważ połączenie między oprogramowaniem a procesorem końcowym jest w środowisku chronionym.

Przewidziana jest aplikacja kliencka, którą można wykorzystywać w obrębie danego państwa członkowskiego do wystosowywania zapytań do rejestrów własnych lub do rejestrów innych państw członkowskich. Klienci będą rozpoznawani przy pomocy nru identyfikacyjnego użytkownika/hasła lub certyfikatu klienta. Połączenie z użytkownikiem może być zaszyfrowane, ale szyfrowanie leży w gestii poszczególnych państw członkowskich.

2.2. *Aspekty bezpieczeństwa dotyczące wymiany wiadomości*

Bezpieczeństwo opiera się na połączeniu protokołu HTTPS i podpisu XML. Rozwiązanie to wykorzystuje podpis XML do podpisywania wszystkich wiadomości przesyłanych na serwer i umożliwia uwierzytelnienie nadawcy wiadomości przez sprawdzenie podpisu. Jednostronny SSL (tylko certyfikat serwera) jest używany w celu ochrony poufności i integralności przesyłanej wiadomości i daje ochronę przed atakami przez skreślenie/powtórzenie i wstawienie. Zamiast opracowywania oprogramowania na specjalne zamówienie w celu wdrożenia dwustronnego SSL, wprowadza się podpis XML. Korzystanie z tego podpisu jest bliższe usługom sieciowym niż dwustronny SSL i wobec tego ma większe znaczenie strategiczne.

Podpis XML można wprowadzić kilkoma sposobami, ale wybranym tu sposobem jest wykorzystywanie podpisu XML jako elementu zapewniania bezpieczeństwa usług internetowych (WSS). WSS precyzuje sposób korzystania z podpisu XML. Ponieważ WSS opiera się na normie SOAP, logiczne jest możliwie jak najściślejsze stosowanie się do tej normy.

2.3. *Aspekty bezpieczeństwa niedotyczące wymiany wiadomości*

2.3.1. Zatwierdzanie użytkowników

Użytkownicy oprogramowania sieciowego EUCARIS uwierzytelniają się przez nazwę użytkownika i hasło. Ponieważ wykorzystywane jest standardowe uwierzytelnienie z systemu Windows, państwa członkowskie mogą podwyższyć standard uwierzytelnienia w razie potrzeby przez zastosowanie certyfikatów klientów.

2.3.2. Role użytkowników

Oprogramowanie EUCARIS wspomaga różne role użytkowników. Każdy klaster usług ma własną autoryzację. Np. (wyłączni) użytkownicy funkcji „Traktat EUCARIS" nie mogą korzystać z funkcji „Prüm". Funkcje administratorów są oddzielone od regularnych funkcji użytkowników końcowych.

2.3.3. Rejestrowanie i śledzenie wymiany wiadomości

Oprogramowanie EUCARIS ułatwia rejestrowanie wszystkich rodzajów wiadomości. Funkcja administratora umożliwia administratorowi krajowemu ustalenie, które wiadomości są zarejestrowane – wnioski od użytkowników końcowych, wnioski przychodzące od innych państw członkowskich, informacje przekazywane z rejestrów krajowych itp.

Oprogramowanie można skonfigurować, tak by wykorzystywało do tej rejestracji wewnętrzną bazę danych lub bazę zewnętrzną (Oracle). Decyzja o tym, jakie wiadomości mają być rejestrowane, zależy wyraźnie od możliwości rejestracji w innych częściach dotychczasowych systemów i połączonych z nimi aplikacji klientów.

Nagłówek każdej wiadomości zawiera informacje o składających wniosek państwie członkowskim, organizacji w tym państwie oraz użytkowniku. Zaznaczona jest także przyczyna złożenia wniosku.

Przez połączoną rejestrację w państwie członkowskim składającym wniosek i odpowiadającym możliwe jest dokładne śledzenie każdej wiadomości (np. wniosku od obywatela).

Rejestracja jest konfigurowana przez system sieci klienta EUCARIS (menu Administracja, konfiguracja rejestracji). Funkcję rejestracji wykonuje System Centralny. Gdy rejestrowanie jest uruchomione, w jednym zapisie dotyczącym rejestracji przechowywana jest cała wiadomość (nagłówek i treść). Poziom rejestracji można ustalić według określonej usługi i według rodzaju wiadomości przechodzącej przez system główny.

Poziomy rejestracji

Możliwe są następujące poziomy rejestracji:

Prywatny – wiadomość jest zarejestrowana: rejestracja NIE jest dostępna dla usługi extract logging, ale jest dostępna jedynie na szczeblu krajowym do celów audytu i rozwiązywania problemów.

Brak – wiadomość nie jest w ogóle rejestrowana.

Rodzaje wiadomości

Wymiana informacji między państwami członkowskimi składa się z kilku wiadomości, których schematy przedstawione są poniżej.

Rodzaje wiadomości są, jak następuje (na rysunku dotyczą systemu podstawowego EUCARIS w państwie członkowskim X):

1. Wniosek skierowany do głównego systemu_wniosek od klienta
2. Wniosek skierowany do innego państwa członkowskiego_wniosek o wiadomość od systemu głównego tego państwa członkowskiego
3. Wniosek do systemu głównego tego państwa członkowskiego_wniosek o wiadomość z systemu głównego innego państwa członkowskiego
4. Wniosek do dotychczasowego rejestru_wiadomość z systemu głównego
5. Wniosek skierowany do głównego systemu_wniosek o wiadomość z dotychczasowego rejestru
6. Odpowiedź z głównego systemu_wniosek klienta o wiadomość
7. Odpowiedź innego państwa członkowskiego_wniosek o wiadomość z systemu głównego tego państwa członkowskiego
8. Odpowiedź od systemu głównego tego państwa członkowskiego_wniosek o wiadomość z innego państwa członkowskiego
9. Wniosek od dotychczasowego rejestru_wniosek o wiadomość z systemu głównego
10. Odpowiedź z głównego systemu_wniosek o wiadomość z dotychczasowego rejestru

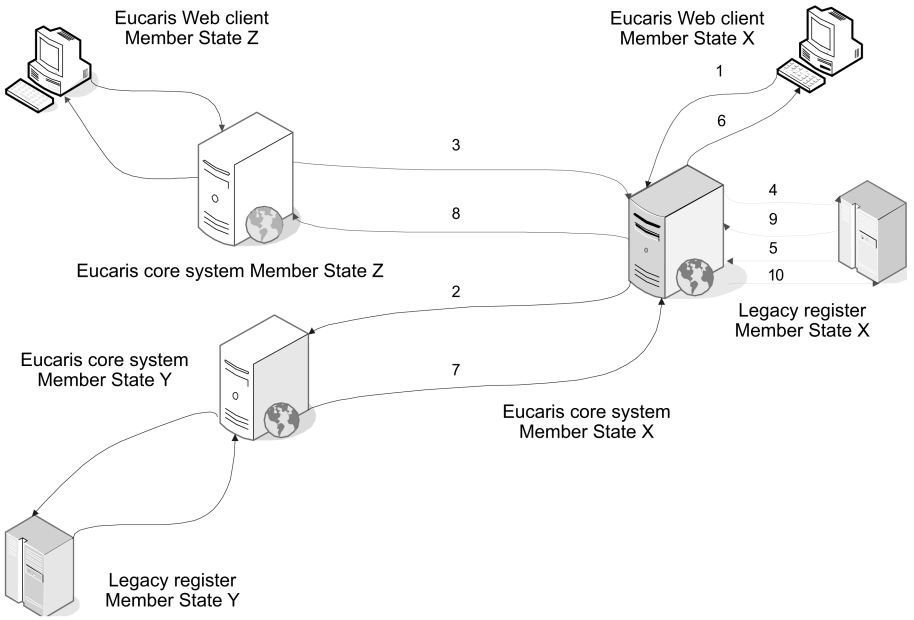
Rysunek przedstawia następujące ścieżki wymiany informacji:

— wniosek o informacje od państwa członkowskiego X do państwa członkowskiego Y – niebieskie strzałki. Wniosek ten i odpowiedź na niego składają się, odpowiednio, z wiadomości typu 1, 2, 7 i 6,

— wniosek o informacje od państwa członkowskiego Z do państwa członkowskiego X – czerwone strzałki. Wniosek ten i odpowiedź na niego składają się, odpowiednio, z wiadomości typu 3, 4, 9 i 8,

— wniosek o informacje z dotychczasowego rejestru do jego systemu głównego (ścieżka ta obejmuje także wniosek od klienta korzystającego z dotychczasowego systemu) – zielone strzałki. Na ten rodzaj wniosku składają się wiadomości typu 5 i 10.

Rysunek. Rodzaje rejestrowanych wiadomości



2.3.4. Moduł bezpieczeństwa sprzętu

Nie stosuje się modułu bezpieczeństwa sprzętu.

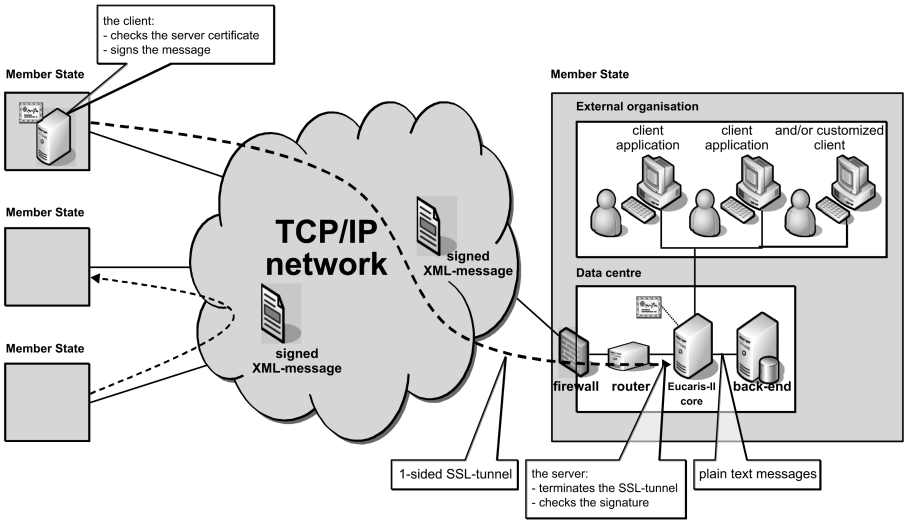
Moduł bezpieczeństwa sprzętu daje dobrą ochronę dla klucza stosowanego do podpisywania wiadomości oraz do identyfikacji serwerów. Podwyższa to ogólny poziom bezpieczeństwa, lecz moduł taki jest kosztowny w zakupie/utrzymaniu, a nie ma wymogów stosowania FIPS 140-2 poziom 2 lub modułu na poziomie 3. Ponieważ wykorzystywana jest zamknięta sieć, która skutecznie łagodzi zagrożenia, postanawia się nie stosować początkowo modułu bezpieczeństwa. Jeżeli moduł ten jest niezbędny do np. uzyskania akredytacji, można włączyć go do architektury systemu.

3. *Warunki techniczne wymiany danych*

3.1. *Ogólny opis oprogramowania EUCARIS*

3.1.1. Zarys

Oprogramowanie EUCARIS łączy wszystkie uczestniczące państwa członkowskie w sieć, w której każde państwo członkowskie komunikuje się bezpośrednio z innymi. Nie ma centralnego komponentu, który byłby potrzebny do nawiązania łączności. Oprogramowanie EUCARIS prowadzi bezpieczną łączność z innymi państwami członkowskimi i przekazuje wiadomości do procesora końcowego dotychczasowych systemów państw członkowskich, wykorzystując XML. Architekturę tę pokazuje poniższy rysunek.



Państwa członkowskie wymieniają wiadomości przez bezpośrednie przesyłanie ich do odbiorcy. Ośrodek danych danego państwa członkowskiego jest podłączony do sieci wykorzystywanej do wymiany wiadomości (TESTA). Aby dostać się do sieci TESTA, państwa członkowskie podłączają się do niej przez krajowy węzeł sieci. Do podłączenia do sieci wykorzystywana jest zapora ogniowa, a oprogramowanie EUCARIS jest podłączone do tego zabezpieczenia przez router. W zależności od rozwiązania wybranego do ochrony wiadomości, certyfikat jest stosowany przez router lub przez oprogramowanie EUCARIS.

Przewidziana jest aplikacja kliencka, którą można wykorzystywać w obrębie danego państwa członkowskiego do wystosowywania zapytań do rejestrów własnych lub do rejestrów innych państw członkowskich. Aplikacja ta jest podłączona do EUCARIS. Klienci będą identyfikowani za pomocą ID użytkownika/hasła lub certyfikatu klienta. Połączenie z użytkownikiem z organizacji zewnętrznej (np. policji) może być zaszyfrowane, ale szyfrowanie leży w gestii poszczególnych państw członkowskich.

3.1.2. Zakres systemu

Zakres zastosowania systemu EUCARIS ogranicza się do procesów mających udział w wymianie informacji między organami rejestracyjnymi w państwach członkowskich oraz do podstawowej prezentacji tych informacji. Procedury oraz zautomatyzowane procesy, w których należy zastosować te informacje, znajdują się poza zakresem zastosowania systemu.

Państwa członkowskie mogą postanowić o stosowaniu funkcji klienta EUCARIS lub o utworzeniu własnej aplikacji klienckiej. Tabela poniżej opisuje te aspekty systemu EUCARIS, z których korzystanie jest obowiązkowe lub zalecane, oraz te, z których korzystanie nie jest obowiązkowe lub może być ustalone przez państwa członkowskie.

Aspekty EUCARIS	M/O [1]	Uwagi
Koncepcja sieci	M	Koncepcja zakłada łączność „każdego z każdym”
Sieć fizyczna	M	TESTA
Oprogramowanie podstawowe	M	Oprogramowanie podstawowe EUCARIS musi być zastosowane do połączenia z pozostałymi państwami członkowskimi. Oferuje ono następujące funkcje: — szyfrowanie i podpisywanie wiadomości, — sprawdzanie tożsamości nadawcy, — uprawnienia przyznane państwom członkowskim i użytkownikom lokalnym, — routing wiadomości, — tworzenie kolejek wiadomości asynchronicznych, jeżeli odbiorca jest chwilowo niedostępny, — funkcja kierowania zapytań do wielu krajów, — rejestracja wymiany wiadomości, — przechowywanie wiadomości przychodzących.
Oprogramowanie klienta	O	Oprócz oprogramowania podstawowego państwo członkowskie może wykorzystywać oprogramowanie klienta EUCARIS II. W miarę potrzeby oprogramowania podstawowe i klienta są modyfikowane pod kontrolą organizacji EUCARIS.
Koncepcja bezpieczeństwa	M	Koncepcja opiera się na podpisach XML za pomocą certyfikatów klientów i na szyfrowaniu w trybie SSL za pomocą certyfikatów obsługi.
Specyfikacja wiadomości	M	Każde państwo członkowskie musi stosować się do specyfikacji wiadomości ustalonych przez organizację EUCARIS i niniejszą decyzję Rady. Specyfikacje może zmienić wyłącznie organizacja EUCARIS w porozumieniu z państwami członkowskimi.
Obsługa i wsparcie	M	Przyjęcie nowych państw członkowskich lub nowej funkcji leży w gestii organizacji EUCARIS. Funkcje bieżącego nadzoru i pomocy są centralnie zarządzane przez wyznaczone do tego państwo członkowskie.

[1] M = obowiązkowe korzystanie lub zgodność; O = nieobowiązkowe korzystanie lub zgodność.

3.2. *Wymogi funkcjonalne i pozafunkcjonalne*

3.2.1. Funkcje ogólne

W niniejszej sekcji opisano w sposób podstawowy główne funkcje ogólne.

Nr	Opis
1.	System umożliwia organom rejestracyjnym państw członkowskich wymianę wiadomości – wniosków i odpowiedzi – w sposób interaktywny.
2.	System zawiera aplikację kliencką umożliwiającą użytkownikom końcowym przesyłanie wniosków i przedstawianie odpowiedzi do przetwarzania ręcznego.
3.	System ułatwia „transmitowanie", umożliwiając w ten sposób danemu państwu członkowskiemu przesyłanie wniosku do wszystkich pozostałych. Oprogramowanie podstawowe konsoliduje odpowiedzi przychodzące w jedną wiadomość przekazywaną do aplikacji klienckiej (funkcja ta ma nazwę „Zapytanie do wielu krajów").
4.	System jest w stanie obsługiwać różne rodzaje wiadomości. Role użytkowników, autoryzacja, routing, podpisywanie i rejestrowanie są zdefiniowane według konkretnej usługi.
5.	System umożliwia państwom członkowskim wymianę partii wiadomości lub wiadomości zawierających dużą liczbę wniosków lub odpowiedzi. Wiadomości te są obsługiwane w sposób asynchroniczny.
6.	System ustawia wiadomości asynchroniczne w kolejce, jeżeli państwo członkowskie będące odbiorcą jest chwilowo niedostępne, i gwarantuje dostarczenie wiadomości, gdy tylko odbiorca jest ponownie dostępny.
7.	System przechowuje przychodzące wiadomości asynchroniczne do czasu, kiedy mogą one być przetworzone.
8.	System udostępnia tylko programy EUCARIS należące do innych państw członkowskich, nie zaś do indywidualnych organizacji znajdujących się w tych państwach, tj. każdy organ rejestracyjny stanowi jedyny pomost między krajowymi użytkownikami końcowymi a odpowiednimi organami w innych państwach członkowskich.
9.	Możliwe jest określenie użytkowników z różnych państw członkowskich na serwerze EUCARIS i ich autoryzacja zgodnie z prawami tego państwa członkowskiego.
10.	Wiadomości zawierają informacje dotyczące państwa członkowskiego występującego z wnioskiem, organizacji i użytkownika końcowego.
11.	System ułatwia rejestrację wymiany wiadomości między różnymi państwami członkowskimi i między oprogramowaniem podstawowym a krajowymi systemami rejestracji.
12.	System umożliwia organizacji lub państwu członkowskiemu wyznaczonym do tego zadania gromadzenie zarejestrowanych informacji na temat wiadomości wysłanych/otrzymanych przez wszystkie uczestniczące państwa członkowskie do celów sporządzania sprawozdań statystycznych.
13.	Każde państwo członkowskie samo zaznacza, jakie zarejestrowane informacje są udostępniane wyznaczonemu organowi, a jakie są „prywatne".
14.	System umożliwia administratorom krajowym każdego państwa członkowskiego sporządzania wyciągów użytecznych danych statystycznych.
15.	System umożliwia dodanie nowych państw członkowskich na drodze prostych procedur administracyjnych.

3.2.2. Użyteczność

Nr	Opis
16.	System zapewnia interfejs do zautomatyzowanego przetwarzania wiadomości przez systemy procesorów końcowych/systemy dotychczasowe i umożliwia wprowadzenie interfejsu użytkownika do tych systemów (indywidualnie dostosowany interfejs użytkownika).
17.	Obsługi systemu można się łatwo nauczyć, system jest jasny i zawiera teksty pomocy.
18.	System posiada dokumentację wspomagającą państwa członkowskie w działaniach integrujących, operacyjnych i przyszłej konserwacji (np. instrukcje, dokumentacja funkcjonalna i techniczna, instrukcja operacyjna…).
19.	Interfejs użytkownika jest wielojęzyczny i oferuje użytkownikowi końcowemu możliwość wybrania języka.
20.	Interfejs użytkownika zawiera udogodnienia dla administratora lokalnego umożliwiające przetłumaczenie pozycji na ekranie i kodowanych informacji na język danego kraju.

3.2.3. Niezawodność

Nr	Opis
21.	System jest zaprojektowany jako solidny i niezawodny system operacyjny, odporny na błędy obsługujących i zdolny do bezproblemowej regeneracji po przerwach w dostawie prądu i innych zdarzeniach. Ponowne uruchomienie systemu bez utraty danych lub z minimalną utratą musi być możliwe.
22.	System musi dawać stabilne i możliwe do odtworzenia rezultaty.
23.	System został zaprojektowany do niezawodnego funkcjonowania. Można go wdrożyć w konfiguracji gwarantującej 98-procentową dostępność (przez redundancję, wykorzystanie serwerów zapasowych itd.) w każdym przypadku komunikacji dwustronnej.
24.	Możliwe jest użytkowanie części systemu, nawet podczas awarii niektórych komponentów (jeżeli państwo członkowskie C ma awarię, państwa A i B nadal mogą się komunikować). Należy zminimalizować liczbę pojedynczych punktów awarii w łańcuchu informacji.
25.	Czas powrotu do sprawności systemu po poważnej awarii powinien wynosić mniej niż jeden dzień. Powinna istnieć możliwość zminimalizowania czasu wyłączenia z pracy, wykorzystując możliwość zdalnej pomocy, np. z centralnego biura obsługi.

3.2.4. Wydajność

Nr	Opis
26.	System może być używany 24 h na dobę/7 dni w tygodniu. Ramy czasowe są wtedy także wymagane od dotychczasowych systemów w państwach członkowskich.
27.	System szybko reaguje na wnioski użytkowników bez względu na inne zadania wykonywane w tym samym czasie. Jest to także wymagane od dotychczasowych systemów stron w celu zapewnienia odpowiedniego czasu reakcji. Dopuszczalny jest ogólny czas reakcji wynoszący maksymalnie 10 sekund dla pojedynczego wniosku.
28.	System został zaprojektowany dla wielu użytkowników i w taki sposób, że zadania w tle mogą być wykonywane, podczas gdy użytkownik wykonuje zadania bieżące.
29.	System został zaprojektowany tak, by można było go rozszerzyć w przypadku zwiększenia liczby wiadomości w następstwie wprowadzenia nowej funkcji lub dołączenia nowych organizacji lub nowych państw członkowskich.

3.2.5. Bezpieczeństwo

Nr	Opis
30.	System nadaje się (np. w zakresie środków bezpieczeństwa) do wymiany informacji zawierających dane osobowe wymagające szczególnej ochrony (np. dane właściciela/posiadacza samochodu), opatrzone klauzulą zastrzeżenia UE.
31.	System jest utrzymywany tak, tak że uniemożliwiony jest nieupoważniony dostęp do danych.
32.	System zawiera moduł umożliwiający bieżący nadzór nad prawami i zezwoleniami krajowych użytkowników końcowych.
33.	Państwa członkowskie mogą sprawdzić tożsamość nadawcy (na szczeblu państwa członkowskiego) przez podpisy XML.
34.	Państwa członkowskie muszą wyraźnie upoważnić inne państwa członkowskie do żądania konkretnych informacji.
35.	Na poziomie oprogramowania system zapewnia całościowy zestaw zabezpieczeń i szyfrów zgodny z poziomem bezpieczeństwa wymaganym w takich sytuacjach. Wyłączność i integralność informacji gwarantuje podpis XML i szyfrowanie drogą tunelowania SSL.
36.	Wszelka wymiana wiadomości może być prześledzona przez rejestrację.
37.	Zapewniona jest ochrona przed atakami polegającymi na usuwaniu wiadomości (wiadomość usuwana jest przez stronę trzecią) i atakami polegającymi na wprowadzaniu lub powtarzaniu wiadomości.
38.	System wykorzystuje certyfikaty zaufanej strony trzeciej (trusted third party – TTP).
39.	System może obsługiwać różne certyfikaty pochodzące z jednego państwa członkowskiego, w zależności od rodzaju wiadomości lub usługi.

Nr	Opis
40.	Środki bezpieczeństwa na szczeblu oprogramowania są wystarczające, aby umożliwić korzystanie z sieci nieakredytowanych.
41.	System jest w stanie wykorzystywać nowe technologie zabezpieczeń, takie jak zapora ogniowa XML.

3.2.6. Możliwość dostosowania

Nr	Opis
42.	System daje możliwość rozszerzenia go o nowe rodzaje wiadomości i nowe funkcje. Koszty adaptacji są minimalne z racji scentralizowanego opracowywania komponentów oprogramowania.
43.	Państwa członkowskie mają możliwość określenia nowych rodzajów wiadomości do użytku dwustronnego. Nie wszystkie państwa członkowskie muszą uwzględniać wszystkie rodzaje wiadomości.

3.2.7. Wsparcie i konserwacja

Nr	Opis
44.	System zapewnia możliwość bieżącego nadzoru centralnemu punktowi obsługi lub operatorom w odniesieniu do sieci i serwerów w różnych państwach członkowskich.
45.	System umożliwia zdalne wspomaganie przez centralny punkt obsługi.
46.	System umożliwia analizowanie problemów.
47.	System można rozszerzyć na nowe państwa członkowskie.
48.	Oprogramowanie może być łatwo zainstalowane przez personel mający minimalną wiedzę i doświadczenie w dziedzinie technologii informacyjnych. Procedura instalacji jest w jak największym stopniu zautomatyzowana.
49.	System zapewnia stałe środowisko testowe i akceptacyjne.
50.	Roczne koszty utrzymania i wsparcia zostały zminimalizowane dzięki przestrzeganiu norm rynkowych i utworzeniu programu w taki sposób, aby wymagał możliwie jak najmniejszego wsparcia ze strony centralnego punktu obsługi.

3.2.8. Wymogi projektowe

Nr	Opis
51.	System jest zaprojektowany i posiada dokumentację z założeniem wieloletniego okresu użytkowania.
52.	System został tak zaprojektowany, by był niezależny od dostawcy sieci.
53.	System jest kompatybilny z aktualnym sprzętem i oprogramowaniem wykorzystywanymi w państwach członkowskich, gdyż współpracuje z tymi systemami rejestracji wykorzystując standardową, otwartą technologię usług sieciowych (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 itd.)

3.2.9. Stosowne normy

Nr	Opis
54.	System jest zgodny z wymogami ochrony danych określonymi w rozporządzeniu (WE) nr 45/2001 (art. 21, 22 i 23) i dyrektywie 95/46/WE.
55.	System jest zgodny z normami wymiany danych pomiędzy administracjami (IDA).
56.	System współpracuje z UTF8.

Rozdział 4: **Ocena**

1. ***Procedura oceny zgodnie z art. 20 (opracowanie decyzji zgodne z art. 25 ust. 2 decyzji Rady 2008/615/WSiSW)***

1.1. *Kwestionariusz*

Odpowiednia grupa robocza Rady opracowuje kwestionariusz dotyczący każdej z zautomatyzowanych metod wymiany danych przedstawionych w rozdziale 2 decyzji 2008/615/WSiSW.

Gdy państwo członkowskie uzna, że spełnia wymogi dotyczące wymiany danych w odpowiedniej kategorii, wypełnia odpowiedni kwestionariusz.

1.2. *Operacja pilotażowa*

W celu dokonania oceny wyników kwestionariusza państwo członkowskie pragnące rozpocząć wymianę danych przeprowadza operację pilotażową wraz z państwem członkowskim (lub ich większą liczbą), które już prowadzi wymianę danych w ramach decyzji Rady. Operacja pilotażowa odbywa się niedługo przed inspekcją lub wkrótce po niej.

Warunki i ustalenia dotyczące operacji pilotażowej określi odpowiednia grupa robocza Rady i będą one oparte na uprzednim indywidualnym ustaleniu z danym państwem członkowskim. Państwa członkowskie biorące udział w operacji pilotażowej uzgodnią szczegóły praktyczne.

1.3. *Wizyta ewaluacyjna*

W celu dokonania oceny wyników kwestionariusza w państwie członkowskim pragnącym rozpocząć wymianę danych zostanie przeprowadzona inspekcja.

Warunki i ustalenia dotyczące inspekcji określi odpowiednia grupa robocza i będą one oparte na uprzednich indywidualnych ustaleniach poczynionych między danym państwem członkowskim a zespołem inspekcyjnym. Dane państwo członkowskie umożliwi zespołowi inspekcyjnemu sprawdzenie zautomatyzowanej wymiany danych w kategorii lub kategoriach, które mają być ocenione, w szczególności przez opracowanie harmonogramu inspekcji uwzględniającego wnioski zespołu.

W ciągu jednego miesiąca zespół inspekcyjny sporządzi sprawozdanie z inspekcji i przekaże je danemu państwu członkowskiemu, tak by mogło ono wyrazić swoje uwagi. W razie potrzeby sprawozdanie zostanie zmienione przez zespół na podstawie uwag przekazanych z państwa członkowskiego.

W skład zespołu inspekcyjnego wejdą eksperci w liczbie nie większej niż 3, wyznaczeni przez państwa członkowskie biorące udział w zautomatyzowanej wymianie danych w kategoriach podlegających ocenie, mający doświadczenie w odniesieniu do danej kategorii danych, posiadający odpowiednie krajowe poświadczenie bezpieczeństwa osobowego umożliwiające zajmowanie się tymi sprawami i zgadzający się na udział w co najmniej jednej inspekcji w innym państwie członkowskim. Komisja zostanie poproszona o wyznaczenie przedstawiciela, który dołączy do zespołu w charakterze obserwatora.

Członkowie zespołu inspekcyjnego będą respektowali poufny charakter informacji, które uzyskają przy wykonywaniu swoich zadań.

1.4. *Sprawozdanie dla Rady*

Zgodnie z art. 25 ust. 2 decyzji 2008/615/WSiSW Rada otrzyma, w celu podjęcia decyzji, ogólne sprawozdanie z oceny podsumowujące wyniki kwestionariuszy, inspekcję i operację pilotażową.

2. ***Procedura oceny zgodnie z art. 21***

2.1. *Dane statystyczne i sprawozdanie*

Każde państwo członkowskie będzie gromadziło dane statystyczne dotyczące wyników zautomatyzowanej wymiany danych. W celu zapewnienia porównywalności model statystyczny zostanie opracowany przez odpowiednią grupę roboczą.

Te dane statystyczne będą corocznie przekazywane Sekretariatowi Generalnemu, który opracuje podsumowanie za dany rok, oraz Komisji.

Oprócz tego państwa członkowskie będą regularnie proszone, ale najwyżej raz w roku, o dalsze informacje o administracyjnych, technicznych i finansowych aspektach wdrażania zautomatyzowanej wymiany danych, w miarę potrzeby, w celu analizowania i ulepszania tej procedury. Na podstawie tych informacji zostanie opracowane sprawozdanie dla Rady.

2.2. *Korekta*

W racjonalnym okresie czasu Rada przeanalizuje opisaną tutaj metodę inspekcji i zrewiduje ją w razie potrzeby.

3. Spotkania ekspertów

W ramach posiedzeń odpowiedniej grupy roboczej Rady będą odbywały się regularne spotkania ekspertów w celu organizowania i wprowadzania w życie wyżej wymienionych procedur oceny oraz w celu dzielenia się doświadczeniami i omawiania ewentualnych ulepszeń. W miarę potrzeby wyniki tych dyskusji ekspertów zostaną wprowadzone do sprawozdania, o którym mowa w pkt 2.1 powyżej.