

# Az Európai Unió Hivatalos Lapja

# L 210

Magyar nyelvű kiadás

## Jogszabályok

51. évfolyam

2008. augusztus 6.

Tartalom

### III Az EU-Szerződés alapján elfogadott jogi aktusok

#### AZ EU-SZERZŐDÉS VI. CÍME ALAPJÁN ELFOGADOTT JOGI AKTUSOK

- ★ A Tanács 2008/615/IB határozata (2008. június 23.) a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről 1
- ★ A Tanács 2008/616/IB határozata (2008. június 23.) a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB határozat végrehajtásáról ..... 12
- ★ A Tanács 2008/617/IB határozata (2008. június 23.) az Európai Unió tagállamainak különleges intervenciók egységei közötti együttműködés javításáról válsághelyzetekben ..... 73

Ár: 18 EUR

# HU

Azok a jogi aktusok, amelyek címe normál szedéssel jelenik meg, a mezőgazdasági ügyek napi intézésére vonatkoznak, és rendszerint csak korlátozott ideig maradnak hatályban.

Valamennyi más jogszabály címét vastagon szedik, és előtte csillag szerepel.

## III

(Az EU-Szerződés alapján elfogadott jogi aktusok)

## AZ EU-SZERZŐDÉS VI. CÍME ALAPJÁN ELFOGADOTT JOGI AKTUSOK

## A TANÁCS 2008/615/IB HATÁROZATA

(2008. június 23.)

**a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről**

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unióról szóló szerződésre és különösen annak 30. cikke (1) bekezdésének a) és b) pontjára, 31. cikke (1) bekezdésének a) pontjára, 32. cikkére és 34. cikke (2) bekezdésének c) pontjára,

tekintettel a Belga Királyság, a Bolgár Köztársaság, a Német Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság, az Osztrák Köztársaság, a Szlovén Köztársaság, a Szlovák Köztársaság, az Olasz Köztársaság, a Finn Köztársaság, a Portugál Köztársaság, Románia és a Svéd Köztársaság kezdeményezésére,

tekintettel az Európai Parlament véleményére <sup>(1)</sup>,

mivel:

- (1) A Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között létrejött, különösen a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló szerződés (a Prümi Szerződés) hatálybalépését követően e kezdeményezés előterjesztésére – a Bizottsággal való konzultációt követően, az Európai Unióról szóló szerződés rendelkezéseivel összhangban – abból a célból kerül sor, hogy a Prümi Szerződés rendelkezéseinek tartalmát beépítsék az Európai Unió jogi keretrendszerébe.
- (2) Az Európai Tanács 1999. októberi tamperei ülésének következtetése megerősítették, hogy a bűncselekmények felderítése és kivizsgálása céljából fokozottabb információ-cserére van szükség a tagállamok illetékes hatóságai között.
- (3) A 2004 novemberében elfogadott, az Európai Unióban a szabadság, a biztonság és a jog érvényesülése megerősítéséről szóló hágai programban az Európai Tanács

kinyilvánította azon meggyőződését, hogy e cél érdekében innovatív megközelítésre van szükség a bűnüldözéssel kapcsolatos információk határokon átnyúló cseréje terén.

- (4) Az Európai Tanács ennek megfelelően megállapította, hogy ezen információk cseréjének meg kell felelnie a hozzáférhetőség elvére vonatkozó feltételeknek. Ez azt jelenti, hogy amennyiben egy bűnüldözési tisztviselőnek az Unió egyik tagállamában feladatainak végrehajtásához információkra van szüksége, megkaphatja azokat egy másik tagállamból, és a másik tagállam azon bűnüldözési hatóságai, amelyeknek a szóban forgó információk a birtokában vannak, a kérvényezett célra rendelkezésre fogják azokat bocsátani, figyelembe véve az adott tagállamban zajló nyomozások szükségleteit.
- (5) Az Európai Tanács 2008. január 1-jében határozta meg a hágai program e célkitűzésének elérésére vonatkozó határidőt.
- (6) Az Európai Unió tagállamainak bűnüldözési hatóságai közötti, információk és bűnüldözési operatív információk cseréjének leegyszerűsítéséről szóló, 2006. december 18-i 2006/960/IB tanácsi kerethatározat <sup>(2)</sup> már meghatározza azokat a szabályokat, amelyek szerint a tagállamok bűnüldözési hatóságai a bünyügyi nyomozás vagy bűnüldözési operatív műveletek végrehajtása céljából gyorsan és hatékonyan kicserélhetik a meglévő információkat és bűnüldözési operatív információkat.
- (7) A szabadság, a biztonság és a jog érvényesülésének erősítéséről szóló hágai program szintén kimondja, hogy az új technológiákat teljes mértékben fel kell használni, és a nemzeti adatbázisokhoz is kölcsönösen biztosítani kell a hozzáférést, és előírja egyúttal, hogy új, központosított európai adatbázisokat kell létrehozni azon tanulmányok alapján, amelyek igazolták, hogy azok hozzáadott értéket képviselnek.

<sup>(1)</sup> 2007. június 10-i vélemény (a Hivatalos Lapban még nem tették közzé).

<sup>(2)</sup> HL L 386., 2006.12.29., 89. o.

- (8) A hatékony nemzetközi együttműködés szempontjából alapvető fontosságú, hogy gyorsan és hatékonyan kerülhessen sor pontos információk kicserélésére. A cél olyan eljárások bevezetése, amelyek révén elősegíthető a gyors, hatékony és költségkímélő adatszerezeszközök alkalmazása. Az adatok közös felhasználása keretében ezen eljárásokban érvényesülnie kell az elszámoltathatóságnak, valamint azoknak megfelelő garanciákat kell tartalmazniuk az adatok pontosságára és biztonságára vonatkozóan a továbbítás és tárolás során, továbbá tartalmazniuk kell az adatszere rögzítésére és az átadott információk felhasználási korlátozásaira vonatkozó eljárásokat.
- (9) A Prümi Szerződés teljesíti ezeket a követelményeket. Annak érdekében, hogy minden tagállam vonatkozásában teljesülhessenek a hágai program alapvető követelményei, a program által meghatározott időkeretben, a Prümi Szerződés lényegi részei tartalmának alkalmazása minden tagállamra nézve kötelezővé kell, hogy váljon.
- (10) E határozat ennél fogva olyan, a Prümi Szerződés főbb rendelkezésein alapuló és az információcsere javítására irányuló rendelkezéseket tartalmaz, amelyek alapján a tagállamok hozzáférést biztosítanak egymás számára automatizált DNS-elemzési állományaikhoz, automatizált daktiloszkópiai azonosítási rendszereikhez és gépjárműnyilvántartási adataikhoz. A nemzeti DNS-elemzési állományokból és automatizált daktiloszkópiai azonosítási rendszerekből származó adatok esetében a „találat/nincs találat” rendszernek lehetővé kell tennie a keresést végző tagállam számára, hogy – második lépésként – az adott dokumentációhoz kapcsolódó konkrét személyes adatokat kérjen az azt kezelő tagállamtól, és szükség esetén a kölcsönös segítségnyújtási eljárások – többek között a 2006/960/IB kerethatározat alapján elfogadott eljárások – révén további információkat kérjen.
- (11) Ez jelentősen felgyorsítja a jelenlegi eljárásokat azáltal, hogy a tagállamok számára láthatóvá válik, hogy van-e olyan másik tagállam – és ha van, melyik az –, amely rendelkezik a számára szükséges információkkal.
- (12) A határokon átnyúló adat-összehasonlítás várhatóan új dimenziót nyit majd a bűnözéssel szembeni küzdelemben. Az adatok összehasonlítása révén szerzett információk új nyomozási megközelítéseket nyithatnak meg a tagállamok számára, és így kulcsfontosságú szerepet játszhatnak a tagállami bűnüldöző szervek és igazságügyi hatóságok segítésében.
- (13) A szabályok a tagállamok nemzeti adatbázisainak hálózatba kapcsolásán alapulnak.
- (14) Bizonyos feltételek mellett lehetővé kell tenni a tagállamok számára a személyes és nem személyes adatok átadását a határon átnyúló dimenzióval rendelkező nagyszabású eseményekkel kapcsolatos, a bűncselekmények megelőzése, valamint a közrend és a közbiztonság fenntartása céljából való információcsere javítása érdekében.
- (15) A 12. cikk alkalmazásában a tagállamok határozhatnak úgy, hogy elsőbbséget biztosítanak a súlyos bűncselekmények elleni küzdelemnek, szem előtt tartva az adattovábbításhoz rendelkezésre álló korlátozott technikai kapacitást.
- (16) Az információcsere javítása mellett szükség van a rendőri szervek közötti szorosabb együttműködés egyéb formáinak szabályozására is, különösen közös biztonsági műveletek (pl. közös járőrszolgálatok) révén.
- (17) A büntetőügyekben folytatott szorosabb rendőrségi és igazságügyi együttműködéshez szorosan kapcsolódnia kell az alapvető jogok tiszteletben tartásának, különösen a magánélet és a személyes adatok védelme tiszteletben tartása jogának, amelyet különleges adatvédelmi szabályokkal kell garantálni, amelyeknek igazodniuk kell az adatszere különböző formáinak egyedi jellegéhez. Az ilyen adatvédelmi rendelkezéseknek figyelembe kell venniük különösen az adatbázisokhoz való, határokon átnyúló, online hozzáférés egyedi jellegét. Mivel az online hozzáférés esetében a dokumentációt kezelő tagállamnak nem áll módjában előzetes ellenőrzést végezni, gondoskodni kell egy utólagos ellenőrzést biztosító rendszerről.
- (18) A „találat/nincs találat” rendszer struktúráját ad az anonim profilok összehasonlításához, amelynek esetében a további személyes adatok cseréjére csak találatot követően kerül sor, és amely adatok átadására és átvételére a nemzeti jog az irányadó, a jogsegélyre vonatkozó szabályokat is beleértve. Ez a megoldás megfelelő adatvédelmi rendszert biztosít, leszögezve, hogy a személyes adatok más tagállamnak való átadása megfelelő szintű adatvédelmet igényel a fogadó tagállam részéről.
- (19) A szorosabb rendőrségi és igazságügyi együttműködésből következő átfogó információ- és adatszere figyelemmel ez a határozat megfelelő szintű adatvédelem biztosítására törekszik. Figyelembe veszi a személyes adatok feldolgozására vonatkozóan az Európa Tanácsnak az egyének személyes adataik gépi feldolgozása során való védelméről szóló, 1981. január 28-i egyezményében és az egyezmény 2001. november 8-i kiegészítő jegyzőkönyvében megállapított védelmi szintet, valamint az Európa Tanácsnak a személyes adatoknak a rendőrségi ágazatban való felhasználása szabályozására irányuló R (87) 15. ajánlásában megfogalmazott elveket.

- (20) Az e határozatban található adatvédelmi rendelkezések olyan adatvédelmi elveket is tartalmaznak, amelyek a harmadik pillérbeli adatvédelemről szóló kerethatározat hiányában szükségesek. Ezt a kerethatározatot a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés egész területére alkalmazni kell, azzal a feltétellel, hogy adatvédelmi szintje nem alacsonyabb, mint az Európa Tanácsnak az egyének személyes adataik gépi feldolgozása során való védelméről szóló, 1981. január 28-i egyezményében és annak 2001. november 8-i kiegészítő jegyzőkönyvében megállapított védelem, valamint a kerethatározat figyelembe veszi a Miniszteri Bizottságnak a tagállamoknak szóló, a személyes adatoknak a rendőrségi ágazatban való felhasználása szabályozására irányuló, 1987. szeptember 17-i R (87) 15. ajánlását, abban az esetben is, ha az adatok feldolgozása nem gépi úton történik.
- (21) Mivel e határozat céljait, nevezetesen az Európai Unión belüli információcsere javítását a tagállamok egymástól elszigetelten nem tudják kielégítően megvalósítani a bűnözéssel szembeni küzdelem és a biztonsági ügyek határon átnyúló jellegéből adódóan, és ezekben az ügyekben rászorulnak egymás munkájának alapul vételére, ezért azok európai uniós szinten jobban megvalósíthatók, a Tanács intézkedéseket hozhat az Európai Közösség létrehozásáról szóló szerződés 5. cikkében meghatározottak szerinti szubszidiaritás elvének megfelelően, amelyre az Európai Unióról szóló szerződés 2. cikke hivatkozik. Az EK-Szerződés 5. cikkében meghatározott arányosság elvének megfelelően e határozat nem lépi túl az e célkitűzések eléréséhez szükséges mértéket.
- (22) E határozat tiszteletben tartja azokat az alapvető jogokat és megfelel azoknak az alapelveknek, amelyeket különösen az Európai Unió alapjogi chartája ismer el,

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

## 1. FEJEZET

### ÁLTALÁNOS SZEMPONTOK

#### 1. cikk

#### Cél és hatály

A tagállamok e határozat által meg akarják erősíteni a Szerződés VI. címe által szabályozott ügyekben folytatott határokon átnyúló együttműködést és különösen a bűncselekmények megelőzéséért és kivizsgálásáért felelős hatóságok közötti információcserét. E cél érdekében e határozat az alábbi területekre vonatkozóan tartalmaz szabályokat:

- a) a DNS-profilok, daktiloszkópiai adatok és bizonyos nemzeti gépjármű-nyilvántartási adatok automatizált továbbítására vonatkozó feltételekkel és eljárásokkal kapcsolatos rendelkezések (2. fejezet);
- b) a határon átnyúló dimenzióval rendelkező nagyszabású eseményekkel kapcsolatos adatok átadásának feltételeire vonatkozó rendelkezések (3. fejezet);

- c) a terrorcselekmények megelőzése érdekében történő információátadás feltételeire vonatkozó rendelkezések (4. fejezet);
- d) a határon átnyúló rendőrségi együttműködés különböző intézkedésekkel való megerősítésére vonatkozó feltételekkel és eljárásokkal kapcsolatos rendelkezések (5. fejezet).

## 2. FEJEZET

### ONLINE HOZZÁFÉRÉSI ÉS NYOMONKÖVETÉSI KÉRÉSEK

#### 1. SZAKASZ

#### DNS-profilok

##### 2. cikk

#### Nemzeti DNS-elemzési állományok létrehozása

- (1) A tagállamok nemzeti DNS-elemzési állományokat nyitnak és vezetnek a bűncselekmények tekintetében végzett nyomozás céljára. Az ezen állományokban tárolt adatok e határozat keretében történő feldolgozását e határozat rendelkezéseivel összhangban, a feldolgozásra vonatkozó nemzeti jog betartásával kell végrehajtani.
- (2) E határozat végrehajtása érdekében a tagállamok biztosítják az (1) bekezdés első mondatában említett nemzeti DNS-elemzési állományokból származó referenciaadatok rendelkezésre állását. A referenciaadatok kizárólag a DNS nem kódoló szakaszai alapján létrehozott DNS-profilokat és egy hivatkozási számot tartalmaznak. A referenciaadatok nem tartalmazhatnak olyan adatokat, amelyek alapján az adatalany közvetlenül azonosítható. A konkrét személyekhez nem kapcsolható referenciaadatok (nem azonosított DNS-profilok) e minőségének felismerhetőnek kell lennie.

- (3) Minden egyes tagállam a 36. cikkel összhangban tájékoztatja a Tanács Főtitkárságát azokról a nemzeti DNS-elemzési állományokról, amelyekre a 2–6. cikk vonatkozik, valamint a 3. cikk (1) bekezdésében említett automatizált keresés feltételeiről.

##### 3. cikk

#### DNS-profilok automatizált keresése

- (1) Bűncselekmények esetében folytatott nyomozások érdekében a tagállamok lehetővé teszik más tagállamok – 6. cikkben említett – nemzeti kapcsolattartó pontjai számára a DNS-elemzési állományaikban lévő referenciaadatokhoz való hozzáférést, és felhatalmazzák őket a DNS-profilok összehasonlításával történő automatizált keresés végzésére. Keresést csak egyedi esetekben és a keresést végző tagállam nemzeti jogával összhangban lehet folytatni.

- (2) Amennyiben az automatizált keresés eredményeként valamely átadott DNS-profil egyezést mutat a fogadó tagállam állományában rögzített DNS-profilokkal, a keresést végző tagállam nemzeti kapcsolattartó pontja automatizált módon megkapja azokat a referenciaadatokot, amelyek alapján a találatot elérték. Egyezés hiányában a kapcsolattartó egy arról szóló automatizált értesítést kap.

## 4. cikk

**DNS-profilok automatizált összehasonlítása**

(1) Bűncselekmények esetében folytatott nyomozások érdekében a tagállamok kölcsönös beleegyezés alapján és nemzeti kapcsolattartó pontjaikon keresztül összehasonlítják azonosítatlan DNS-profiljaikat az egyéb nemzeti DNS-elemzési állományok referenciaadatain alapuló valamennyi DNS-profillal. A profilokat automatizált módon kell átadni és összehasonlítani. Azonosítatlan DNS-profilokat összehasonlítás céljára kizárólag akkor kell átadni, amennyiben arról a megkereső tagállam nemzeti joga rendelkezik.

(2) Amennyiben valamely tagállam az (1) bekezdésben említett összehasonlítás eredményeként úgy találja, hogy a részére átadott DNS-profilok bármelyike megegyezik valamely, a saját DNS-elemzési állományában lévővel, haladéktalanul átadja a másik tagállam kapcsolattartó pontjának azokat a referenciaadatokat, amelyek alapján az egyezést találták.

## 5. cikk

**További személyes adatok és egyéb információk átadása**

Amennyiben a 3. és 4. cikkben említett eljárás DNS-profilok egyezését mutatja, a referenciaadatokkal kapcsolatos további rendelkezésre álló személyes adatok és egyéb információk átadására a megkeresett tagállam nemzeti joga az irányadó, a jogsegélyre vonatkozó szabályokat is beleértve.

## 6. cikk

**Nemzeti kapcsolattartó pont és végrehajtási intézkedések**

(1) A 3. és 4. cikkben említett adatok átadása céljából minden egyes tagállam nemzeti kapcsolattartó pontot jelöl ki. A nemzeti kapcsolattartó pont hatáskörére az alkalmazandó nemzeti jog az irányadó.

(2) A 3. és 4. cikkben meghatározott eljárásokra vonatkozó technikai rendelkezések részleteit a 33. cikkben említett végrehajtási intézkedések tartalmazzák.

## 7. cikk

**Sejtanyagok gyűjtése és DNS-profilok átadása**

Amennyiben folyamatban lévő nyomozások vagy büntetőeljárások során valamely – a megkeresett tagállam területén tartózkodó – konkrét személy tekintetében nem áll rendelkezésre DNS-profil a megkeresett tagállam területén, a megkeresett tagállam az érintett személytől származó sejtanyag gyűjtését és vizsgálatát, valamint az így kapott DNS-profil átadását magában foglaló jogsegélyt nyújt, amennyiben

- a) a megkereső tagállam meghatározza a kérelem célját;
- b) a megkereső tagállam saját jogának megfelelően nyomozást elrendelő határozatot vagy az illetékes hatóság által kiadott

nyilatkozatot mutat be, amely igazolja, hogy a sejtanyag gyűjtésére és vizsgálatára vonatkozó követelmények teljesülnek, amennyiben az érintett személy a megkereső tagállam területén tartózkodna; és

- c) a megkeresett tagállam joga szerint a sejtanyag gyűjtésére és vizsgálatára, valamint az így kapott DNS-profil átadására vonatkozó követelmények teljesülnek.

## 2. SZAKASZ

**Daktiloszkópiai adatok**

## 8. cikk

**Daktiloszkópiai adatok**

E határozat végrehajtása érdekében a tagállamok biztosítják a bűncselekmények megelőzése és kivizsgálása céljából létrehozott nemzeti automatizált ujjlenyomat-azonosító rendszer állományából származó referenciaadatok rendelkezésre állását. A referenciaadatok csak az ujjlenyomatok adatait és egy hivatkozási számot tartalmaznak. A referenciaadatok nem tartalmazhatnak olyan adatokat, amelyek alapján az adatalany közvetlenül azonosítható. A konkrét személyekhez nem kapcsolható referenciaadatok (nem azonosított daktiloszkópiai adatok) e minőségük felismerhetőnek kell lennie.

## 9. cikk

**Daktiloszkópiai adatok automatizált keresése**

(1) Bűncselekmények megelőzése és vizsgálata érdekében a tagállamok lehetővé teszik más tagállamok – 11. cikkben említett – nemzeti kapcsolattartó pontjai számára az általuk e célra létrehozott automatizált daktiloszkópiai azonosító rendszerben lévő referenciaadatokhoz való hozzáférést, és felhatalmazzák őket daktiloszkópiai adatok összehasonlításával történő automatizált keresés végzésére. Keresést csak egyedi esetekben és a keresést végző tagállam nemzeti jogával összhangban lehet folytatni.

(2) Daktiloszkópiai adatoknak az állományt kezelő tagállam kezelésében lévő referenciaadatokkal való megfelelésének megerősítését a fogadó tagállam nemzeti kapcsolattartó pontja végzi az egyértelmű egyezéshez szükséges referenciaadatok automatizált átadása révén.

## 10. cikk

**További személyes adatok és egyéb információk átadása**

Amennyiben a 9. cikkben említett eljárás daktiloszkópiai adatok egyezését mutatja, a referenciaadatokkal kapcsolatos további rendelkezésre álló személyes adatok és egyéb információk átadására a megkeresett tagállam nemzeti joga az irányadó, a jogsegélyre vonatkozó szabályokat is beleértve.

## 11. cikk

**Nemzeti kapcsolattartó pont és végrehajtási intézkedések**

(1) A 9. cikkben említett adatok átadása céljából minden egyes tagállam nemzeti kapcsolattartó pontot jelöl ki. A nemzeti kapcsolattartó pont hatáskörére az alkalmazandó nemzeti jog az irányadó.

(2) A 9. cikkben meghatározott eljárásra vonatkozó technikai rendelkezések részleteit a 33. cikkben említett végrehajtási intézkedések tartalmazzák.

## 3. SZAKASZ

**Gépjármű-nyilvántartási adatok**

## 12. cikk

**Gépjármű-nyilvántartási adatok automatizált keresése**

(1) Bűncselekmények megelőzése és vizsgálata, valamint a keresést végző tagállam bíróságainak vagy ügyészségi hatóságainak a hatáskörébe tartozó egyéb jogsértések kezelése, továbbá a közbiztonság fenntartása érdekében a tagállamok lehetővé teszik más tagállamok – (2) bekezdésben említett – nemzeti kapcsolattartó pontjai számára az alábbi nemzeti gépjármű-nyilvántartási adatokhoz való hozzáférést, és felhatalmazzák őket egyedi esetekben automatizált keresés végzésére:

- a) tulajdonosokra vagy üzemeltetőkre vonatkozó adatok; és
- b) gépjárművekre vonatkozó adatok.

Keresés kizárólag teljes alvázsám vagy teljes rendszám alapján végezhető. Keresést csak a keresést végző tagállam nemzeti jogával összhangban lehet folytatni.

(2) Az (1) bekezdésben említett adatok átadása céljából minden egyes tagállam kijelöl egy beérkező kérelmekkel foglalkozó nemzeti kapcsolattartó pontot. A nemzeti kapcsolattartó pont hatáskörére az alkalmazandó nemzeti jog az irányadó. Az eljárásra vonatkozó technikai rendelkezések részleteit a 33. cikkben említett végrehajtási intézkedések tartalmazzák.

## 3. FEJEZET

**NAGYSZABÁSÚ ESEMÉNYEK**

## 13. cikk

**Nem személyes adatok átadása**

Bűncselekmények megelőzése, valamint határon átnyúló dimenziójú, nagyszabású események – különösen sportrendezvények vagy az Európai Tanács ülései – során a közrend és biztonság fenntartása érdekében a tagállamok kérelemre, illetve saját

kezdeményezésükre és az átadó tagállam nemzeti jogának megfelelően átadják egymás részére az e célból szükséges nem személyes adatokat.

## 14. cikk

**Személyes adatok átadása**

(1) Bűncselekmények megelőzése, valamint határon átnyúló dimenziójú, nagyszabású események – különösen sportrendezvények vagy az Európai Tanács ülései – során a közrend és biztonság fenntartása érdekében a tagállamok kérelemre, illetve saját kezdeményezésükre és az átadó tagállam nemzeti jogának megfelelően – ha az az ilyen adatok átadását lehetővé teszi – személyes adatokat adnak át egymás részére, amennyiben jogerős ítélet vagy egyéb körülmények alapján arra lehet következtetni, hogy az adatalányok az eseményeken bűncselekményt fognak elkövetni vagy veszélyt jelentenek a közrendre és a biztonságra.

(2) Személyes adatok kizárólag az (1) bekezdésben meghatározott célok, és az adatátadás tárgyát képező konkrét események tekintetében dolgozhatók fel. Az átadott adatokat az (1) bekezdésben említett célok elérését követően vagy ha azok már nem elérhetők, haladéktalanul törölni kell. Az átadott adatokat legkésőbb egy év elteltével minden esetben törölni kell.

## 15. cikk

**Nemzeti kapcsolattartó pont**

A 13. és 14. cikkben említett adatok átadása céljából minden egyes tagállam nemzeti kapcsolattartó pontot jelöl ki. A nemzeti kapcsolattartó pont hatáskörére az alkalmazandó nemzeti jog az irányadó.

## 4. FEJEZET

**TERRORCSELEKMÉNYEK MEGAKADÁLYOZÁSÁRA IRÁNYULÓ INTÉZKEDÉSEK**

## 16. cikk

**Információk átadása terrorcselekmények megakadályozása érdekében**

(1) Terrorcselekmények megakadályozása érdekében a tagállamok egyedi esetekben, nemzeti joguknak megfelelően, – akár kérelem hiányában is – a (2) bekezdésben meghatározott személyes adatokat és információkat adhatnak át más tagállamok (3) bekezdésben említett nemzeti kapcsolattartó pontjai számára, amennyiben ez azért szükséges, mert bizonyos körülmények alapján joggal feltételezhető, hogy az adatalány a terrorizmus elleni küzdelemről szóló, 2002. június 13-i 2002/475/IB tanácsi kerethatározat <sup>(1)</sup> 1–3. cikkében említett bűncselekményeket fog elkövetni.

<sup>(1)</sup> HL L 164., 2002.6.22., 3. o.

(2) Az átadandó adatok magukban foglalják a vezetéknevet, keresztnéve(ke)t, a születési helyet és a születési időt, valamint az (1) bekezdésben említett feltételezés kialakulásához vezető körülmények leírását.

(3) Minden egyes tagállam nemzeti kapcsolattartó pontot jelöl ki a más tagállamok nemzeti kapcsolattartó pontjaival való információcseré céljából. A nemzeti kapcsolattartó pont hatáskörére az alkalmazandó nemzeti jog az irányadó.

(4) Az átadó tagállam a nemzeti jognak megfelelően meghatározhatja az ilyen adatok és információk átvevő tagállam általi felhasználásának feltételeit. Az átvevő tagállam köteles ezen feltételeket betartani.

## 5. FEJEZET

### AZ EGYÜTTMŰKÖDÉS EGYÉB FORMÁI

#### 17. cikk

#### Közös műveletek

(1) A rendőrségi együttműködés megerősítése érdekében a tagállamok által kijelölt illetékes hatóságok a közrend és a biztonság fenntartása, valamint a bűncselekmények megelőzése érdekében közös őrzőjáratokat és egyéb közös műveleteket hajthatnak végre, amelyekben a tagállamok által kijelölt tisztviselők vagy egyéb állami alkalmazottak (a továbbiakban: tisztviselők) vesznek részt valamely másik tagállam területén végrehajtott műveletekben.

(2) Fogadó tagállamként és saját nemzeti jogával összhangban, valamint a kirendelő tagállam hozzájárulásával minden egyes tagállam végrehajtó hatáskörrel ruházhatja fel a kirendelő tagállam közös műveletben részt vevő tisztviselőit, vagy – amennyiben a fogadó tagállam joga azt lehetővé teszi – lehetővé teheti a kirendelő tagállamok tisztviselői számára, hogy a végrehajtó hatáskörüket a kirendelő tagállam jogának megfelelően gyakorolják. Az ilyen végrehajtó hatáskört kizárólag a fogadó tagállam felügyelete mellett és – főszabályként – tisztviselőinek jelenlétében lehet gyakorolni. A kirendelő tagállamok tisztviselői a fogadó tagállam nemzeti jogának hatálya alá tartoznak. A fogadó tagállam felelősséggel tartozik tevékenységükért.

(3) A kirendelő tagállam közös műveletekben részt vevő tisztviselőinek követniük kell a fogadó tagállam illetékes hatósága által adott utasításokat.

(4) A tagállamok benyújtják a 36. cikkben említett nyilatkozatot, amelyben meghatározzák az együttműködés gyakorlati szempontjait.

#### 18. cikk

#### Nagy tömegeket vonzó eseményekkel, katasztrófákkal és súlyos balesetekkel kapcsolatos segítségnyújtás

A tagállamok illetékes hatóságai kölcsönösen segítséget nyújtanak egymásnak, a nemzeti joggal összhangban, nagy tömegeket

vonzó eseményekkel és hasonló nagyszabású eseményekkel, katasztrófákkal, valamint súlyos balesetekkel kapcsolatosan, azáltal, hogy törekednek megelőzni a bűncselekményeket, és fenntartani a közrendet és a biztonságot

a) egymás lehető leghamarabb történő értesítésével az ilyen határokon átnyúló hatásokkal járó eseményekről, valamint a vonatkozó információk cseréjével;

b) saját területükön a szükséges rendőrségi intézkedések meghozatalával és összehangolásával a határokon átnyúló hatásokkal járó események esetén;

c) lehetséges mértékben tisztviselők, szakértők és tanácsadók küldésével, valamint felszerelés biztosításával azon tagállam kérelmére, amelynek területén az esemény bekövetkezett.

#### 19. cikk

#### Fegyver, lőszer és egyéb felszerelés használata

(1) A kirendelő tagállam azon tisztviselői, akik a 17. vagy a 18. cikk alapján részt vesznek egy másik tagállam területén zajló közös műveletben, annak során viselhetik nemzeti egyenruhájukat. Maguknál tarthatják továbbá az őket kirendelő tagállam nemzeti joga szerint számukra engedélyezett fegyvereket, lőszert és egyéb felszerelést. A fogadó tagállam megtilthatja egyes fegyverek, lőszer vagy felszerelés viselését valamely kirendelő tagállam tisztviselői számára.

(2) A tagállamok benyújtják a 36. cikkben említett nyilatkozatokat, amelyben felsorolják azokat a fegyvereket, lőszert és egyéb felszerelést, amelyeket kizárólag jogos önvédelemre vagy mások védelmére lehet használni. A fogadó tagállamnak a művelet tényleges irányítását végző tisztviselője egyedi esetekben – a nemzeti jognak megfelelően – engedélyezheti a fegyvereknek, a lőszernek és a felszerelésnek az első mondatban meghatározottakat meghaladó használatát is. A fegyverek, lőszer és felszerelés használatára a fogadó tagállam joga az irányadó. Az illetékes hatóságok tájékoztatják egymást az engedélyezett fegyverekről, lőszerről és felszerelésről, valamint azok használatának feltételeiről.

(3) Amennyiben valamely tagállam tisztviselői az e határozat keretében folytatott intézkedés során valamely másik tagállam területén gépjárműveket vesznek igénybe, ugyanazon közúti közlekedési szabályok hatálya alá tartoznak, mint a fogadó tagállam tisztviselői, az elsőbbségadásra és a különös kiváltságokra vonatkozó szabályokat is beleértve.

(4) A tagállamok benyújtják a 36. cikkben említett nyilatkozatokat, amelyekben meghatározzák a fegyverek, lőszer és felszerelés használatának gyakorlati szempontjait.

## 20. cikk

**Védelem és segítségnyújtás**

A tagállamok kötelesek más tagállamok határokat átlépő tisztviselői számára azok feladatai ellátása során a saját tisztviselőik részére biztosítottal megegyező védelmet és segítséget nyújtani.

## 21. cikk

**A polgári felelősségre vonatkozó általános szabályok**

(1) Amikor valamely tagállam tisztviselői a 17. cikk alapján egy másik tagállam területén tevékenykednek, tagállamuk az általuk eljárásuk során okozott károkért annak a tagállamnak a joga szerint felel, amelynek területén e tevékenységet végzik.

(2) Az a tagállam, amelynek területén az (1) bekezdésben említett kár bekövetkezett, a kárt ugyanolyan feltételek mellett téríti meg, mintha azt a saját tisztviselői okozták volna.

(3) Az (1) bekezdésben meghatározott esetben az a tagállam, amelynek tisztviselői egy másik tagállam területén valakinek kárt okoztak, teljes mértékben megtéríti ez utóbbi tagállamnak az általa a károsultaknak, illetve a károsult személyek jogán jogosult más személyeknek kifizetett kártérítés összegét.

(4) Amikor valamely tagállam tisztviselői a 18. cikk alapján egy másik tagállam területén tevékenykednek, ez utóbbi tagállam az általuk eljárásuk során okozott károkért nemzeti joga szerint felel.

(5) Amennyiben a (4) bekezdésben említett kár súlyos gondatlanság vagy szándékos kötelezettségszegés eredménye, akkor a fogadó tagállam a kirendelő tagállamhoz fordulhat annak érdekében, hogy ez utóbbi visszatérítse számára az általa a sértetteknek vagy a nevükben eljárni jogosult személyeknek kifizetett összegeket.

(6) Az (1) bekezdésben szabályozott esetben — harmadik személyekkel szemben fennálló jogai gyakorlásának sérelme nélkül és a (3) bekezdésben foglalt rendelkezés kivételével — minden tagállam lemond az olyan károk megtérítésének igényléséről, amelyet egy másik tagállamtól szenvedett el.

## 22. cikk

**Büntetőjogi felelősség**

Az e határozat keretében másik tagállam területén tevékenykedő tisztviselők az általuk vagy velük szemben esetleg elkövetett bűncselekmények tekintetében a fogadó tagállam tisztviselőivel azonos elbánásban részesülnek, amennyiben az érintett tagállamokra nézve kötelező bármely más megállapodás másként nem rendelkezik.

## 23. cikk

**Munkaviszony**

Az e határozat keretében másik tagállam területén tevékenykedő tisztviselőkre továbbra is a saját tagállamukban alkalmazandó

munkajogi rendelkezések vonatkoznak, különösen a fegyelmi szabályok tekintetében.

## 6. FEJEZET

**AZ ADATVÉDELEMRE VONATKOZÓ ÁLTALÁNOS RENDELKEZÉSEK**

## 24. cikk

**Fogalommeghatározások és hatály**

(1) E határozat alkalmazásában:

- a) „személyes adatok feldolgozása”: a személyes adatokkal automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, úgymint adatok gyűjtése, rögzítése, rendszerezése, tárolása, átalakítása vagy megváltoztatása, szétválogatása, visszakeresése, az azokba való betekintés, adatok felhasználása, közlése átadás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, adatok összehangolása vagy összekapcsolása, zárolása, törlése vagy megsemmisítése. Az e határozat szerinti feldolgozás magában foglalja továbbá a találatok meglétéről szóló értesítést;
- b) „automatizált keresési eljárás”: egy másik szerv automatizált állományaihoz való közvetlen hozzáférés, amely eljárás során a válasz is teljesen automatizált módon érkezik;
- c) „megjelölés”: a tárolt személyes adatok megjelölése a jövőbeni feldolgozásuk korlátozásának szándéka nélkül;
- d) „zárolás”: a tárolt személyes adatok megjelölése a jövőbeni feldolgozásuk korlátozásának céljából.

(2) Az e határozat keretében továbbított adatokra az alábbi rendelkezések vonatkoznak, amennyiben a megelőző fejezetek másként nem rendelkeznek.

## 25. cikk

**Az adatvédelem szintje**

(1) Az e határozat keretében átadott személyes adatok tekintetében minden tagállam biztosítja nemzeti jogában a személyes adatok védelmének legalább az Európa Tanácsnak az egyének személyes adataik gépi feldolgozása során való védelméről szóló, 1981. január 28-i egyezménye és annak 2001. november 8-i kiegészítő jegyzőkönyve szerinti védelmével megegyező szintjét, és ennek során figyelembe veszi az Európa Tanács Miniszteri Bizottságának a tagállamoknak szóló, a személyes adatoknak a rendőrségi ágazatban való felhasználása szabályozására irányuló, 1987. szeptember 17-i R (87) 15. ajánlását, abban az esetben is, ha az adatok feldolgozása nem automatizált módon történik.

(2) E határozat keretében nem kerülhet sor személyes adatok átadására mindaddig, amíg ezen fejezet rendelkezéseit végre nem hajtották az ilyen adatátadásban érintett tagállamok területeinek nemzeti jogában. A Tanács egyhangúlag határoz arról, hogy e feltétel teljesült-e.



(3) A (2) bekezdés nem vonatkozik azokra a tagállamokra, amelyekben már megkezdődött a személyes adatok e határozatban előírt átadása a Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között létrejött, a különösen a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló, 2005. május 27-i szerződés (Prümi Szerződés) értelmében.

#### 26. cikk

#### Cél

(1) Az átvevő tagállam a személyes adatokat kizárólag az adatok átadásának e határozaton alapuló célja érdekében dolgozhatja fel. Bármilyen más célból való felhasználás csak az állományt kezelő tagállam előzetes engedélyével megengedett, és az kizárólag a fogadó tagállam nemzeti jogának hatálya alá tartozik. Ilyen engedély abban az esetben adható, ha az egyéb célokat szolgáló feldolgozás az állományt kezelő tagállam nemzeti joga szerint megengedett.

(2) A 3., 4. és 9. cikk értelmében átadott adatok feldolgozása a keresést vagy összehasonlítást végző tagállam által kizárólag az alábbiak érdekében engedélyezett:

- a) az összehasonlított DNS-profilok vagy daktiloszkópiái adatok egyezésének megállapítása;
- b) az adatok egyezése esetén jogsegély iránti rendőrségi vagy igazságügyi kérelem előkészítése és benyújtása a nemzeti jognak megfelelően;
- c) a 30. cikk szerinti jegyzőkönyvbe vétel.

Az állományt kezelő tagállam kizárólag akkor dolgozhatja fel a részére a 3., 4. és 9. cikknek megfelelően átadott adatokat, amennyiben az az összehasonlítás, a keresésre való automatizált válaszadás vagy a 30. cikk szerinti jegyzőkönyvbe vétel céljából szükséges. Az átadott adatokat azok összehasonlítását vagy a keresésre való automatizált válaszadást követően haladéktalanul törölni kell, amennyiben nincs szükség azok további, az első albekezdés b) és c) pontjában említett célokat szolgáló feldolgozására.

(3) A 12. cikk értelmében átadott adatokat az állományt kezelő tagállam kizárólag a keresési eljárásokra való automatizált válaszadás vagy a 30. cikkben meghatározott jegyzőkönyvbe vétel céljából használhatja fel. Az átadott adatokat a keresésre való automatizált válaszadást követően haladéktalanul törölni kell, amennyiben nincs szükség azok további, a 30. cikk szerinti jegyzőkönyvbe vétel célját szolgáló feldolgozására. A válaszadás során a keresést végző tagállam az eljárás eredményeként kapott adatokat kizárólag a keresési eljárás során meghatározott célra használhatja fel.

#### 27. cikk

#### Illetékes hatóságok

Az átadott személyes adatok kizárólag a 26. cikkben említett célok elvégzéséért felelős hatóságok, szervek és bíróságok által dolgozhatók fel. Különösen, adatokat más szervek részére csak az átadó tagállam előzetes engedélyével, és kizárólag az átvevő tagállam nemzeti jogának megfelelően lehet átadni.

#### 28. cikk

#### Az adatok pontossága, aktualitása és tárolási ideje

(1) A tagállamoknak biztosítaniuk kell a személyes adatok pontosságát és aktualitását. Ha például a hivatali eljárás során vagy az adatalanytól származó értesítésből kiderül, hogy helytelen adatok vagy olyan adatok kerültek átadásra, amelyeket nem lett volna szabad átadni, erről haladéktalanul értesíteni kell az átvevő tagállamot vagy tagállamokat. Az érintett tagállam vagy tagállamok kötelesek kijavítani vagy törölni az adatokat. Továbbá a helytelennek talált személyes adatokat is ki kell javítani. Ha az átvevő szerv okkal feltételezi, hogy az átadott adatok helytelenek, vagy azokat törölni kellene, akkor erről haladéktalanul tájékoztatnia kell az átadó szervet.

(2) Azokat az adatokat, amelyek pontosságát az adatalany kétségbe vonja, valamint amelyek pontossága vagy pontatlansága nem állapítható meg, a tagállamok nemzeti jogának megfelelően az adatalany kérésére meg kell jelölni. Amennyiben létezik egy ilyen megjelölés, azt a tagállamok nemzeti jogának figyelembevételével kizárólag az adatalany engedélyével vagy az illetékes bíróság vagy a független adatvédelmi hatóság határozata alapján lehet eltávolítani.

(3) Azokat az átadott személyes adatokat, amelyeket nem lett volna szabad átadni vagy átvenni, törölni kell. A jogszerűen átadott és átvett adatokat törölni kell:

- a) ha az adatok nem vagy már nem szükségesek az átadás céljának szempontjából; amennyiben személyes adatok kérés nélkül kerültek átadásra, az átvevő szervnek haladéktalanul ellenőriznie kell, hogy azok szükségesek-e az átadás céljának szempontjából;
- b) az átadó tagállam nemzeti jogában az adatok megőrzése tekintetében megállapított maximális időtartam lejáratát követően, amennyiben az átadó szerv az átvevő szervet az említett maximális időtartamról az adatok átadásakor tájékoztatta.

Amennyiben joggal feltételezhető, hogy az adatok törlése hátrányosan befolyásolná az adatalany érdekeit, az adatokat a nemzeti jog figyelembevételével a törlés helyett zárolni kell. A zárolt adatokat kizárólag arra a célra szabad átadni vagy felhasználni, amely miatt az adatok nem kerültek törlésre.

## 29. cikk

**Az adatvédelem és adatbiztonság biztosítása érdekében hozott technikai és szervezési intézkedések**

(1) Az áadó és az átvevő szervek lépéseket tesznek annak biztosítására, hogy a személyes adatok hatékony védelemben részesüljenek a véletlen vagy jogosulatlan megsemmisítés, véletlen elvesztés, jogosulatlan hozzáférés, jogosulatlan vagy véletlen változtatás és jogosulatlan közzététel ellen.

(2) Az automatizált keresési eljárás technikai kialakításának jellemzőit a 33. cikkben említett végrehajtási intézkedések szabályozzák, amelyek garantálják, hogy:

- a) az adatvédelem és adatbiztonság biztosítása céljából sor kerüljön a technika jelenlegi állásának megfelelő olyan intézkedések meghozatalára, amelyek különösen az adatok titkosságát és sérthetlenségét szavatolják;
- b) általánosan hozzáférhető hálózatok használata esetén az illetékes hatóságok által elismert kódolási és engedélyezési eljárásokat alkalmazzanak; és
- c) a 30. cikk (2), (4) és (5) bekezdésével összhangban ellenőrizhető legyen a keresések megengedhetősége.

## 30. cikk

**Dokumentáció és jegyzőkönyvezés; az automatizált és a nem automatizált átadásra vonatkozó különleges szabályok**

(1) Az átadás megengedhetőségének ellenőrzése érdekében minden tagállam garantálja, hogy az állományt kezelő szerv és a keresést végző szerv a személyes adatok minden egyes nem automatizált átadását és nem automatizált átvételét dokumentálja. A dokumentáció a következő információkat tartalmazza:

- a) az átadás indoka;
- b) az átadott adatok;
- c) az átadás dátuma; és
- d) a keresést végző szerv és az állományt kezelő szerv neve vagy hivatkozási kódja.

(2) A 3., 9. és a 12. cikken alapuló automatizált adatkeresésre és a 4. cikk szerinti automatizált összehasonlításra a következők vonatkoznak:

- a) automatizált kereséseket vagy összehasonlításokat kizárólag a nemzeti kapcsolattartó pontok különleges engedéllyel rendelkező tisztviselői hajthatnak végre. Az automatizált keresések vagy összehasonlítások végrehajtására jogosult

tisztviselők jegyzékét kérésre az (5) bekezdésben említett felügyeleti hatóságok és az egyéb tagállamok rendelkezésére kell bocsátani;

- b) minden tagállam biztosítja, hogy az állományt kezelő szerv és a keresést végző szerv jegyzőkönyvet készítsen a személyes adatok minden egyes átadásáról és átvételéről, a találatról vagy annak hiányáról való értesítést is beleértve. A jegyzőkönyv a következő információkat tartalmazza:
  - i. az átadott adatok;
  - ii. az átadás dátuma és pontos időpontja; és
  - iii. a keresést végző szerv és az állományt kezelő szerv neve vagy hivatkozási kódja.

A keresést végző szerv jegyzőkönyvbe veszi továbbá a keresés vagy az átadás indokát, valamint a keresést végrehajtó tisztviselő és a keresést vagy az átadást elrendelő tisztviselő ismertetőjelét.

(3) A jegyzőkönyvező szerv kérésre haladéktalanul közli a jegyzőkönyvbe vett adatokat az érintett tagállam illetékes adatvédelmi hatóságaival, legkésőbb a kérelem kézhezvételétől számított négy héten belül. A jegyzőkönyvbe vett adatokat kizárólag a következő célokra lehet felhasználni:

- a) az adatvédelem ellenőrzése;
- b) az adatbiztonság biztosítása.

(4) A jegyzőkönyvbe vett adatokat megfelelő intézkedések segítségével védeni kell a nem megfelelő felhasználással és a helytelen felhasználás egyéb formáival szemben, valamint két évig meg kell őrizni azokat. A megőrzési idő lejártá után a jegyzőkönyvbe vett adatokat haladéktalanul törölni kell.

(5) A személyes adatok átadásának vagy átvételének jogi ellenőrzése a tagállamok független adatvédelmi hatóságainak, vagy adott esetben igazságügyi hatóságainak a feladata. A nemzeti jog figyelembevételével bárki felkérheti ezeket a hatóságokat arra, hogy azok ellenőrizzék a személyükre vonatkozó adatok feldolgozásának jogszerűségét. Ezek és a jegyzőkönyvezésért felelős hatóságok az ilyen kérésektől függetlenül az érintett állományok alapján szűrőpróbaszerűen is ellenőrzik az átadás jogszerűségét.

A független adatvédelmi hatóságok ellenőrzés céljából 18 hónapig megőrzik az ilyen ellenőrzések eredményeit. Ezen időtartam lejártá után haladéktalanul törlik ezeket. A nemzeti joggal összhangban minden adatvédelmi hatóság felkérést kaphat egy másik tagállam független adatvédelmi hatóságától hatáskörei gyakorlására. A tagállamok független adatvédelmi hatóságai – különösen a célirányos információk cseréje révén – elvégzik a kölcsönös együttműködéshez szükséges ellenőrzési feladatokat.

## 31. cikk

**Az adatalanyok tájékoztatáshoz és kártérítéshez fűződő jogai**

(1) Az adatalany részére személyazonossága igazolása után a nemzeti jog szerinti adatalany kérésére a nemzeti jog figyelembevételével, indokolatlan költségek nélkül, közérthető formában és elfogadhatatlan késedelem nélkül tájékoztatást kell nyújtani a személye tekintetében feldolgozott adatokról, az adatok eredetéről, az átvevőről vagy az átvevők kategóriáiról, a feldolgozás tervezett céljáról és – amennyiben a nemzeti jog előírja – a feldolgozás jogalapjáról. Ezen túlmenően az adatalanyok jogában áll a téves adatokat kijavíttatni és a jogszerűtlenül feldolgozott adatokat töröltetni. A tagállamok biztosítják továbbá, hogy az adatalany az adatvédelemmel kapcsolatos jogainak megsértése esetén panaszt nyújthat be egy, az emberi jogokról szóló európai egyezmény 6. cikke (1) bekezdésének értelmében vett független bírósághoz vagy törvényszékhez, vagy a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv<sup>(1)</sup> 28. cikkének értelmében vett független felügyelő hatósághoz, valamint biztosítják, hogy az adatalanyok lehetősége legyen arra, hogy kártérítést követeljen, vagy egyéb típusú jogi elégtétellel éljen. Az ezen jogok érvényesítésére irányuló eljárás részleteire és a tájékoztatáshoz való jog korlátozásának indokaira azon tagállam vonatkozó nemzeti jogi rendelkezései az irányadóak, amelyekben az adatalany jogait érvényesíti.

(2) Amennyiben valamely tagállam egy szerve e határozat értelmében személyes adatot adott át, a másik tagállam fogadó szervezete nem használhatja fel az átadott adatok pontatlanságát jogalapként a sértett féllel szembeni, nemzeti jog szerinti felelőssége elhárításához. Ha a tévesen továbbított adatok felhasználása miatt az átvevő szervvel szemben kártérítést ítélnék meg, a kártérítésként kifizetett összeget az adatokat átadó szerv teljes mértékben megtéríti az átvevő szervnek.

## 32. cikk

**A tagállamok által kért információ**

Az átvevő tagállam kérelemre tájékoztatja az átadó tagállamot az átadott adatok feldolgozásáról és az ezáltal elért eredményekről.

## 7. FEJEZET

**VÉGREHAJTÁSI ÉS ZÁRÓ RENDELKEZÉSEK**

## 33. cikk

**Végrehajtási intézkedések**

A Tanács – minősített többséggel és az Európai Parlamenttel folytatott konzultációt követően – elfogadja az e határozat uniós szintű végrehajtásához szükséges intézkedéseket.

<sup>(1)</sup> HL L 281., 1995.11.23., 31. o. A legutóbb az 1882/2003/EK rendelettel (HL L 284., 2003.10.31., 1. o.) módosított irányelv.

## 34. cikk

**Költségek**

Minden egyes tagállam viseli az e határozat alkalmazásával kapcsolatosan saját hatóságai számára felmerülő műveleti költségeket. Különleges esetekben az érintett tagállamok eltérő szabályozást fogadhatnak el.

## 35. cikk

**Más jogi eszközökkel való kapcsolat**

(1) Az érintett tagállamokra e határozat vonatkozó rendelkezéseit kell alkalmazni a Prümi Szerződésben foglalt megfelelő rendelkezések helyett. A Prümi Szerződés bármilyen egyéb rendelkezését alkalmazni kell a Prümi Szerződés szerződő felei között.

(2) A Szerződés VI. címe alapján elfogadott egyéb aktusokban vállalt kötelezettségeik sérelme nélkül:

a) a tagállamok továbbra is alkalmazhatják a határon átnyúló együttműködésre vonatkozó, e határozat elfogadásának időpontjában érvényben lévő két- vagy többoldalú megállapodásokat vagy megegyezéseket, amennyiben e megállapodások vagy megegyezések nem összeegyeztethetetlenek e határozat célkitűzéseivel;

b) a tagállamok e határozat hatálybalépését követően megköthetnek vagy hatályba léptethetnek határon átnyúló együttműködésre vonatkozó, két- vagy többoldalú megállapodásokat vagy megegyezéseket, amennyiben ezek e határozat céljainak kiterjesztéséről vagy kibővítéséről rendelkeznek.

(3) Az (1) és (2) bekezdésben említett megállapodások és megegyezések nem befolyásolhatják az e megállapodásokban vagy megegyezésekben nem részes tagállamokkal fennálló kapcsolatokat.

(4) A tagállamok e határozat hatálybalépését követően négy héten belül tájékoztatják a Tanácsot és a Bizottságot a (2) bekezdés a) pontja szerinti azon meglévő megállapodásokról és megegyezésekről, amelyeket továbbra is alkalmazni kívánnak.

(5) A tagállamok továbbá tájékoztatják a Tanácsot és a Bizottságot a (2) bekezdés b) pontja szerinti valamennyi új megállapodásról vagy megegyezésről azok aláírását követően három hónapon belül, vagy az e határozat elfogadását megelőzően aláírt eszközök esetében azok hatálybalépését követően három hónapon belül.

(6) E határozat egyetlen rendelkezése sem érinti a tagállamok és harmadik államok közötti két- vagy többoldalú megállapodásokat vagy megegyezéseket.

(7) E határozat nem sérti a jogsegélyre, illetve a bírósági határozatok kölcsönös elismerésére vonatkozó érvényes megállapodásokat.

## 36. cikk

**Végrehajtás és nyilatkozatok**

(1) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy e határozat rendelkezéseinek egy évvel a határozat hatálybalépését követően eleget tegyenek, a 2. fejezet rendelkezéseinek kivételével, amelyek tekintetében a szükséges intézkedéseket három évvel a határozat és az e határozat végrehajtásáról szóló tanácsi határozat hatálybalépését követően kell meghozni.

(2) A tagállamok tájékoztatják a Tanács Főtitkárságát és a Bizottságot arról, hogy az e határozatból eredő kötelezettségeket végrehajtották, és benyújtják az e határozatban előírt nyilatkozatokat. Ennek során az egyes tagállamok jelezhetik, hogy haladéktalanul alkalmazzák e határozatot azoknak a tagállamoknak a viszonylatában, amelyek ugyanilyen közlést tettek.

(3) Az (2) bekezdéssel összhangban tett nyilatkozatokat a Tanács Főtitkárságának továbbított nyilatkozat révén tetszőleges időpontban lehet módosítani. A Tanács Főtitkársága valamennyi kézhez vett nyilatkozatot a tagállamok és a Bizottság rendelkezésére bocsátja.

(4) Ennek és a tagállamok által kérelem alapján szolgáltatott egyéb információk alapján a Bizottság 2012. július 28-ig a Tanács elé terjeszti az e határozat végrehajtásáról szóló jelentését, a további fejlesztésre vonatkozóan általa célszerűnek tartott javaslatokkal együtt.

## 37. cikk

**Alkalmazás**

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Kelt Luxembourgban, 2008. június 23-án.

*a Tanács részéről*

*az elnök*

I. JARC

## A TANÁCS 2008/616/IB HATÁROZATA

(2008. június 23.)

**a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB határozat végrehajtásáról**

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel a 2008/615/IB tanácsi határozat <sup>(1)</sup> 33. cikkére,

tekintettel a Németországi Szövetségi Köztársaság kezdeményezésére,

tekintettel az Európai Parlament véleményére <sup>(2)</sup>,

mivel:

- (1) A Tanács 2008. június 23-án elfogadta a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB határozatot.
- (2) A 2008/615/IB határozat átültette az Európai Unió jogi keretébe a Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között létrejött, a különösen a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló, 2005. május 27-i szerződés (a továbbiakban: a Prümi Szerződés) alapvető elemeit.
- (3) A 2008/615/IB határozat 33. cikke értelmében a Tanácsnak a 2008/615/IB határozat uniós szintű végrehajtásához szükséges intézkedéseket kell elfogadnia az Európai Unióról szóló Szerződés 34. cikke (2) bekezdése c) pontjának második mondatában meghatározott eljárással összhangban. Ezeknek az intézkedéseknek a Prümi Szerződés adminisztratív és technikai végrehajtására és alkalmazására vonatkozó, 2006. december 5-i végrehajtási megállapodáson kell alapulniuk.
- (4) E határozat megállapítja a 2008/615/IB határozatban foglalt együttműködési formák adminisztratív és technikai végrehajtásához elengedhetetlen közös normatív rendelkezéseket. Az e határozat melléklete technikai jellegű végrehajtási rendelkezéseket tartalmaz. A Tanács Főtitkársága ezenkívül kizárólag – a tagállamok által szolgáltatandó – tényszerű információkat tartalmazó külön kézikönyvet fog készíteni és naprakészen tartani.

- (5) A műszaki képességekre tekintettel az új DNS-profilok rutinkeresése elvileg egyszeri kereséssel történik, és erre műszaki szinten megfelelő megoldásokat kell találni,

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

I. FEJEZET

**ÁLTALÁNOS RENDELKEZÉSEK**

1. cikk

**Cél**

E határozat célja a 2008/615/IB határozat végrehajtásához szükséges adminisztratív és technikai rendelkezések megállapítása, különösen a DNS-adatok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok azon határozat 2. fejezete szerinti automatizált cseréjére, valamint az azon határozat 5. fejezetében foglalt, az együttműködés egyéb formáira vonatkozóan.

2. cikk

**Fogalom meghatározások**

E határozat alkalmazásában:

- a) a 2008/615/IB határozat 3., 4. és 9. cikkében említett „keresés” és „összehasonlítás”: a valamely tagállam által átadott DNS-adatok vagy daktiloszkópiai adatok és egy, több vagy valamennyi más tagállam adatbázisaiban tárolt DNS-adatok vagy daktiloszkópiai adatok közötti egyezés megállapítására alkalmazott eljárások;
- b) a 2008/615/IB határozat 12. cikkében említett „automatizált keresés”: egy, több vagy valamennyi tagállam adatbázisaiba való betekintésre alkalmazott on-line hozzáférési eljárás;
- c) „DNS-profil”: az elemzett emberi DNS-minta nem kódoló szakaszának azonosító jellemzőit – azaz a különböző DNS helyeken (lókuszokon) az adott molekuláris szerkezetet – megjelenítő betű- vagy számkód;
- d) „a DNS nem kódoló szakasza”: olyan kromoszóma-régiók, amelyekről genetikai információ nem íródik át, azaz nem ismert, hogy a szervezet funkcionális jellemzőit hordoznak;

<sup>(1)</sup> Lásd e Hivatalos Lap 1. oldalát.

<sup>(2)</sup> A 2008. április 21-i vélemény (a Hivatalos Lapban még nem tették közzé).

- e) „DNS-referenciaadatok”: DNS-profil és egy hivatkozási szám;
- f) „referencia DNS-profil”: azonosított személy DNS-profilja;
- g) „nem azonosított DNS-profil”: bűncselekmények esetén folytatott nyomozások során a nyomokból gyűjtött, és nem azonosított személyhez tartozó DNS-profil;
- h) „megjegyzés”: egy tagállam által nemzeti adatbázisában a DNS-profilon történt bejegyzés, amely azt jelzi, hogy egy másik tagállam által végzett keresés vagy összehasonlítás e DNS-profilra vonatkozóan már egyezést mutatott;
- i) „daktiloszkópiai adatok”: ujjlenyomatok, látens ujjnyomatok, tenyérnyomatok, látens tenyérnyomatok, valamint ezek sablonjai (kódolt ujjlenyomat-jellemzők [*minutiae*]), ha azokat automatizált adatbázisban tárolják és kezelik;
- j) „gépjármű-nyilvántartási adatok”: az e határozat mellékletének 3. fejezetében meghatározott adatok;
- k) a 2008/615/IB határozat 3. cikke (1) bekezdésének második mondatában, 9. cikke (1) bekezdésének második mondatában és 12. cikke (1) bekezdésében említett „egyedi eset” egyetlen nyomozást vagy ügyészégi ügyiratot jelent. Ha egy ilyen állomány egynél több DNS-profil, daktiloszkópiai adatot vagy gépjármű-nyilvántartási adatot tartalmaz, azok egyben, egy kérelemként továbbíthatók.

## 2. FEJEZET

## AZ ADATCSERÉRE VONATKOZÓ KÖZÖS RENDELKEZÉSEK

## 3. cikk

**Műszaki előírások**

A tagállamok a DNS-profilok, a daktiloszkópiai adatok és a gépjármű-nyilvántartási adatok keresésével és összehasonlításával kapcsolatos valamennyi kérelem és válasz tekintetében betartják a közös technikai előírásokat. Ezeket a technikai előírásokat e határozat melléklete tartalmazza.

## 4. cikk

**Kommunikációs hálózat**

A DNS-adatok, daktiloszkópiai adatok és gépjármű-nyilvántartási adatok tagállamok közötti elektronikus cseréje a közigazgatási rendszerek közötti transzeurópai telematikai szolgáltatások kommunikációs hálózatán (TESTA II) és annak további fejlesztésén keresztül történik.

## 5. cikk

**Az automatizált adatcsere hozzáférhetősége**

A tagállamok valamennyi szükséges intézkedést megtesznek annak érdekében, hogy a DNS-adatok, daktiloszkópiai adatok és

gépjármű-nyilvántartási adatok keresése és összehasonlítása a hét minden napjának huszonnégy órájában lehetséges legyen. Műszaki hiba esetén a tagállamok nemzeti kapcsolattartó pontjai haladéktalanul tájékoztatják egymást, és a vonatkozó jogi rendelkezésekkel összhangban az információcsere átmeneti, alternatív módjairól állapodnak meg. Az automatizált adatcserét a lehető leghamarabb helyre kell állítani.

## 6. cikk

**A DNS-adatok és a daktiloszkópiai adatok hivatkozási száma**

A 2008/615/IB határozat 2. és 8. cikkében említett hivatkozási számok az alábbiak kombinációjából állnak:

- a) a tagállamok számára személyes adatoknak és egyéb információknak – egyezés esetén – a 2008/615/IB határozat 5. vagy 10. cikke szerint egy, több vagy valamennyi tagállam részére történő átadása érdekében adatbázisaikban való keresését lehetővé tevő kód;
- b) a DNS-profil vagy a daktiloszkópiai adatok nemzeti eredetét jelölő kód; valamint
- c) a DNS-adatok tekintetében a DNS-profil típusát jelölő kód.

## 3. FEJEZET

## DNS-ADATOK

## 7. cikk

**A DNS-adatok cseréjére vonatkozó elvek**

(1) A DNS-adatok cseréje során a tagállamoknak a meglévő szabványokat kell alkalmazniuk, például az európai szabványt (European Standard Set, ESS) vagy az Interpol-szabványt (Interpol Standard Set of Loci, ISSOL).

(2) A DNS-profilok automatizált keresése és összehasonlítása esetén a továbbításra decentralizált struktúrában kerül sor.

(3) Megfelelő intézkedéseket kell hozni a más tagállamok részére történő adatküldés tárgyát képező adatok bizalmas jellegének és sértetlenségének biztosítása érdekében, beleértve azok kódolását is.

(4) A tagállamok megteszik a szükséges intézkedéseket a többi tagállam számára hozzáférhetővé tett vagy összehasonlítás céljából átadott DNS-profilok sértetlenségének szavatolása érdekében, valamint annak biztosítására, hogy ezen intézkedések megfeleljenek olyan nemzetközi szabványoknak, mint az ISO 17025.

(5) A tagállamok az ISO 3166-1 alpha-2 szabványnak megfelelő tagállami kódokat alkalmaznak.

#### 8. cikk

##### **A DNS-adatokkal kapcsolatos kérelmek és válaszok szabályai**

(1) A 2008/615/IB határozat 3. és 4. cikkében említett automatizált keresésre, illetve automatizált összehasonlításra vonatkozó kérelemnek kizárólag az alábbi információkat kell tartalmaznia:

- a) a kérelmező tagállam tagállami kódja;
- b) a kérelem dátuma, időpontja és száma;
- c) DNS-profilok és hivatkozási számuk;
- d) a továbbított DNS-profilok típusa (nem azonosított DNS-profilok, referencia DNS-profilok); valamint
- e) az adatbázis-rendszerek ellenőrzéséhez és az automatikus keresési folyamatok minőség-ellenőrzéséhez szükséges információk.

(2) Az (1) bekezdésben említett kérelemre küldött válasz (az egyezéstről küldött értesítés) kizárólag az alábbi információkat tartalmazza:

- a) annak feltüntetése, hogy volt-e egy vagy több egyezés (találat) vagy nem volt egyezés (nincs találat);
- b) a kérelem dátuma, időpontja és száma;
- c) a válasz dátuma, időpontja és száma;
- d) a kérelmező és a megkeresett tagállam tagállami kódja;
- e) a kérelmező és a megkeresett tagállam hivatkozási száma;
- f) a továbbított DNS-profilok típusa (nem azonosított DNS-profilok, referencia DNS-profilok);
- g) a kért és az egyező DNS-profilok; valamint
- h) az adatbázis-rendszerek ellenőrzéséhez és az automatikus keresési folyamatok minőség-ellenőrzéséhez szükséges információk.

(3) Automatikus értesítést csak akkor kell küldeni az egyezéstről, ha az automatizált keresés vagy összehasonlítás a lókuszkok egy meghatározott minimuma esetében egyezést eredményezett. Ezt a minimumot e határozat mellékletének 1. fejezete foglalja magában.

(4) A tagállamok biztosítják, hogy a kérelmek összhangban álljanak a 2008/615/IB határozat 2. cikkének (3) bekezdése

értelmében tett nyilatkozatokkal. Ezeknek a nyilatkozatoknak az e határozat 18. cikkének (2) bekezdésében említett kézikönyvben is szerepelniük kell.

#### 9. cikk

##### **A nem azonosított DNS-profiloknak a 2008/615/IB határozat 3. cikke szerinti automatizált kereséséhez kapcsolódó továbbítási eljárás**

(1) Amennyiben egy nem azonosított DNS-profillal végzett keresés a nemzeti adatbázisban nem eredményezett egyezést, vagy nem azonosított DNS-profillal való egyezést eredményezett, a nem azonosított DNS-profilt továbbítani lehet valamennyi egyéb tagállam adatbázisaiba, és amennyiben az ezzel a nem azonosított DNS-profillal végzett keresés egyezést mutat a más tagállamok adatbázisaiban található referencia DNS-profilokkal és/vagy nem azonosított DNS-profilokkal, ezekről az egyezésekről automatikus értesítést kell küldeni és a DNS referenciaadatait továbbítani kell a kérelmező tagállam részére; ha más tagállamok adatbázisaiban nincs egyezés, erről a kérelmező tagállamot automatikusan értesíteni kell.

(2) Ha a nem azonosított DNS-profillal végzett keresés egyezést eredményez más tagállamok adatbázisaiban, minden egyes érintett tagállam nemzeti adatbázisát ilyen értelmű megjegyzéssel egészítheti ki.

#### 10. cikk

##### **A referencia DNS-profiloknak a 2008/615/IB határozat 3. cikke szerint automatizált kereséséhez kapcsolódó továbbítási eljárás**

Amennyiben egy referencia DNS-profillal végzett keresés a nemzeti adatbázisban nem, vagy nem azonosított DNS-profillal eredményezett egyezést, e referencia DNS-profilt valamennyi egyéb tagállam adatbázisaiba továbbítani lehet, és amennyiben az e referencia DNS-profillal végzett keresés egy referencia DNS-profillal és/vagy egy másik nem azonosított DNS-profillal egyezést eredményezett más tagállamok adatbázisaiban, ezen egyezéstről a kérelmező tagállamot automatikusan értesíteni kell, valamint a DNS-referenciaadatokat a részére továbbítani kell; ha más tagállamok adatbázisaiban nincs egyezés, erről a kérelmező tagállamot automatikusan értesíteni kell.

#### 11. cikk

##### **A nem azonosított DNS-profiloknak a 2008/615/IB határozat 4. cikkében említett automatizált összehasonlításához kapcsolódó továbbítási eljárás**

(1) Ha a nem azonosított DNS-profillal végzett összehasonlítás egy referencia DNS-profillal és/vagy egy nem azonosított DNS-profillal egyezést eredményezett más tagállamok adatbázisaiban, ezen egyezésekről a kérelmező tagállamot automatikusan értesíteni kell, valamint a DNS-referenciaadatokat a részére továbbítani kell.

(2) Ha a nem azonosított DNS-profilokkal végzett összehasonlítás egy nem azonosított DNS-profillal vagy egy referencia DNS-profillal egyezést eredményez más tagállamok adatbázisaiban, minden egyes érintett tagállam nemzeti adatbázisát ilyen értelmű megjegyzéssel egészítheti ki.

#### 4. FEJEZET

### DAKTILOSKÓPIAI ADATOK

#### 12. cikk

#### A daktiloszkópiai adatok cseréjére vonatkozó elvek

(1) A daktiloszkópiai adatok digitalizálását és a többi tagállam részére való továbbítását az e határozat mellékletének 2. fejezetében meghatározott egységes adatformátumnak megfelelően kell végezni.

(2) Minden egyes tagállam biztosítja, hogy az általa továbbított daktiloszkópiai adatok minősége az automatizált ujjlenyomat-azonosító rendszerrel (AFIS) végzett összehasonlításhoz megfelelő legyen.

(3) A daktiloszkópiai adatok cseréjére alkalmazandó továbbítási eljárásra decentralizált struktúrában kerül sor.

(4) Megfelelő intézkedéseket kell hozni a más tagállamok részére továbbított daktiloszkópiai adatok bizalmas jellegének és sértetlenségének biztosítása érdekében, beleértve azok kódolását is.

(5) A tagállamok az ISO 3166-1 alpha-2 szabványnak megfelelő tagállami kódokat alkalmaznak.

#### 13. cikk

#### Daktiloszkópiai adatokra vonatkozó keresési kapacitások

(1) Minden tagállam biztosítja, hogy keresési kérelmei ne haladják meg a megkeresett tagállam által meghatározott keresési kapacitásokat. A tagállamok a 18. cikk (2) bekezdésében említett nyilatkozatot nyújtanak be a Tanács Főtitkárságához, amelyben meghatározzák az azonosított és a nem azonosított személyek daktiloszkópiai adataira vonatkozó napi maximális keresési kapacitásukat.

(2) Az adattovábbításonként hitelesítésre elfogadott kérelmek maximális számát e határozat mellékletének 2. fejezete tartalmazza.

#### 14. cikk

#### A daktiloszkópiai adatokkal kapcsolatos kérelmek és válaszok szabályai

(1) A megkeresett tagállam teljesen automatizált eljárással haladéktalanul ellenőrzi a továbbított daktiloszkópiai adatok minőségét. Amennyiben az adatok az automatizált

összehasonlításhoz nem megfelelőek, a megkeresett tagállam késedelem nélkül értesíti a kérelmező tagállamot.

(2) A megkeresett tagállam a kereséseket a kérelmek beérkezésének sorrendjében végzi. A kérelmeket 24 órán belül, teljesen automatizált eljárással fel kell dolgozni. A kérelmező tagállam – ha nemzeti joga ezt előírja – kérheti kérelmeinek gyorsított feldolgozását, amely keresést a megkeresett tagállamnak haladéktalanul el kell végeznie. Ha a határidőket *vis maior* következtében nem lehet betartani, az összehasonlítást az akadályok elhárítását követően haladéktalanul el kell végezni.

#### 5. FEJEZET

### GÉPJÁRMŰ-NYILVÁNTARTÁSI ADATOK

#### 15. cikk

#### A gépjármű-nyilvántartási adatok automatizált keresésének elvei

(1) A gépjármű-nyilvántartási adatok automatizált kereséséhez a tagállamok az Európai Gépjármű és Vezetői Engedély Információs Rendszer (Eucaris) szoftveralkalmazásnak a különösen a 2008/615/IB határozat 12. cikke céljára kifejlesztett változatát, és e szoftver módosított változatait alkalmazzák.

(2) A gépjármű-nyilvántartási adatok automatizált keresésére decentralizált struktúrában kerül sor.

(3) Az Eucaris rendszeren keresztül cserélt információkat kódolt formában kell továbbítani.

(4) A kicserélendő gépjármű-nyilvántartási adatokat e határozat mellékletének 3. fejezete határozza meg.

(5) A 2008/615/IB határozat 12. cikkének végrehajtása során a tagállamok elsőbbséget biztosíthatnak a súlyos bűncselekmények elleni küzdelemhez kapcsolódó kereséseknek.

#### 16. cikk

#### Költségek

Minden egyes tagállam maga viseli a 15. cikk (1) bekezdésében említett Eucaris szoftveralkalmazás kezelése, használata és fenntartása kapcsán felmerülő költségeket.

#### 6. FEJEZET

### RENDŐRSÉGI EGYÜTTMŰKÖDÉS

#### 17. cikk

#### Közös járőrszolgálat és egyéb közös műveletek

(1) A 2008/615/IB határozat 5. fejezetével és különösen az azon határozat 17. cikke (4) bekezdésének, 19. cikke (2) bekezdésének és 19. cikke (4) bekezdésének értelmében benyújtott nyilatkozatokkal összhangban minden egyes tagállam egy vagy



több kapcsolattartót jelöl ki annak lehetővé tétele érdekében, hogy más tagállamok az illetékes hatóságokhoz fordulhassanak, és minden egyes tagállam meghatározhatja a közös járőrszolgálat és az egyéb közös műveletek végrehajtására, és az e műveletekkel, valamint egyéb gyakorlati szempontokkal kapcsolatban más tagállamoktól származó kezdeményezésekre vonatkozó eljárásait, valamint az e műveleteket érintő műveleti szabályokat.

(2) A Tanács Főtitkársága összeállítja és rendszeresen frissíti a kapcsolattartók listáját, és a listában történt bármely változásról tájékoztatja az illetékes hatóságokat.

(3) Az egyes tagállamok illetékes hatóságai kezdeményezést nyújthatnak be közös műveletek végrehajtására. Az adott művelet megkezdése előtt a (2) bekezdésben említett illetékes hatóságok írásbeli vagy szóbeli megállapodásokat kötnek, amelyek olyan részletekre terjedhetnek ki, mint például:

- a) a tagállamoknak a művelet tekintetében illetékes hatóságai;
- b) a művelet konkrét célja;
- c) a műveletnek helyt adó fogadó tagállam;
- d) a fogadó tagállam azon földrajzi területe, ahol a műveletre sor kerül;
- e) a művelet időtartama;
- f) a küldő tagállam(ok) által a fogadó tagállam részére nyújtandó konkrét segítség, beleértve a tiszteket vagy egyéb tisztviselőket, materiális és pénzügyi elemeket;
- g) a műveletben részt vevő tisztek;
- h) a műveletet vezető tiszt;
- i) a küldő tagállam(ok) tisztjei és egyéb tisztviselői által a művelet során a fogadó tagállamban gyakorolható hatáskörök;
- j) a 2008/615/IB határozattal összhangban a kirendelt tisztek által a művelet során használható meghatározott fegyverek, lőszer és felszerelés;
- k) a szállításra, a szállásra és a biztonságra vonatkozó logisztikai szabályok;
- l) a közös művelet költségeinek elosztása, amennyiben az eltér a 2008/615/IB határozat 34. cikkének első mondatában foglaltaktól;
- m) bármely egyéb szükséges elem.

(4) Az e cikkben előírt nyilatkozatok, eljárások és kijelölések a 18. cikk (2) bekezdésében előírt kézikönyvben is szerepelni fognak.

## 7. FEJEZET

### ZÁRÓ RENDELKEZÉSEK

#### 18. cikk

#### Melléklet és kézikönyv

(1) A 2008/615/IB határozat technikai és adminisztratív végrehajtására vonatkozó további részleteket e határozat melléklete állapítja meg.

(2) A Tanács Főtitkársága a 2008/615/IB határozat vagy e határozat alapján tett nyilatkozatokból vagy a Tanács Főtitkárságának részére küldött értesítésekből származó, a kizárólag a tagállamok által nyújtott tényszerű információkat tartalmazó kézikönyvet készít és tart naprakészen. A kézikönyv tanácsi dokumentum formáját fogja öltetni.

#### 19. cikk

#### Független adatvédelmi hatóságok

A tagállamok e határozat 18. cikkének (2) bekezdésével összhangban tájékoztatják a Tanács Főtitkárságát a 2008/615/IB határozat 30. cikkének (5) bekezdésében említett független adatvédelmi hatóságokról vagy igazságügyi hatóságokról.

#### 20. cikk

#### A 2008/615/IB határozat 25. cikkének (2) bekezdésében említett határozatok előkészítése

(1) A Tanács a 2008/615/IB határozat 25. cikkének (2) bekezdésében említettek szerinti határozatot egy kérdőíven alapuló értékelő jelentés alapján hozza meg.

(2) A 2008/615/IB határozat 2. fejezetének megfelelően automatizált adatcsere tekintetében az értékelő jelentés ezenkívül értékelő látogatáson és kísérleti adatcserén fog alapulni, amelyekre akkor kerül sor, miután az érintett tagállam megküldte a Főtitkárság részére a 2008/615/IB határozat 36. cikkének (2) bekezdésében foglalt első mondatnak megfelelő értesítést.

(3) Az eljárás további részleteit e határozat mellékletének 4. fejezete tartalmazza.

#### 21. cikk

#### Az adatcsere értékelése

(1) A 2008/615/IB határozat 2. fejezete szerinti adatcsere adminisztratív, technikai és pénzügyi alkalmazásának, valamint különösen a 15. cikk (5) bekezdésében foglalt mechanizmus alkalmazásának értékelése rendszeres időközönként történik. Az értékelés a 2008/615/IB határozatot az értékelés időpontjában már alkalmazó tagállamokat érinti, és azt azon adatkategóriák

tekintetében kell elvégezni, amelyek vonatkozásában az adatcsere az érintett tagállamok között már megkezdődött. Az értékelés az adott tagállamok jelentésein alapul.

(2) Az eljárás további részleteit e határozat mellékletének 4. fejezete tartalmazza.

22. cikk

**A Prümi Szerződést végrehajtó megállapodással való kapcsolat**

A Prümi Szerződés által kötelezett tagállamoknak az e határozat és annak melléklete teljes körű végrehajtását követően azok vonatkozó rendelkezéseit kell alkalmazniuk a Prümi Szerződést végrehajtó megállapodásban foglalt megfelelő rendelkezések helyett. A végrehajtó megállapodás bármilyen egyéb rendelkezését továbbra is alkalmazni kell a Prümi Szerződés szerződő felei között.

23. cikk

**Végrehajtás**

A tagállamok meghozzák azokat az intézkedéseket, amelyek szükségesek ahhoz, hogy e határozat rendelkezéseinek a 2008/615/IB határozat 36. cikkének (1) bekezdésében említett időszakokon belül megfeleljenek.

24. cikk

**Alkalmazás**

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Kelt Luxembourgban, 2008. június 23-án.

*a Tanács részéről*

*az elnök*

I. JARC

## MELLÉKLET

## TARTALOMJEGYZÉK

## 1. FEJEZET: DNS-adatok cseréje

1. **DNS-sel kapcsolatos bűnügyi technikai kérdések, egyezési szabályok és algoritmusok**

## 1.1. A DNS-profilok jellemzői

## 1.2. Egyezési szabályok

## 1.3. Jelentéstételi szabályok

2. **Tagállami kódszámok táblázata**3. **Funkcionális elemzés**

## 3.1. A rendszer hozzáférhetősége

## 3.2. Második lépés

4. **DNS interfészvezérlési dokumentáció**

## 4.1. Bevezető

## 4.2. Az XML-struktúra meghatározása

5. **Alkalmazási, biztonsági és kommunikációs architektúra**

## 5.1. Áttekintés

## 5.2. Felső szintű architektúra

## 5.3. Biztonsági szabványok és adatvédelem

## 5.4. A rejtjelezési mechanizmushoz használandó protokollok és szabványok: s/MIME és kapcsolódó csomagok

## 5.5. Alkalmazási architektúra

## 5.6. A rejtjelezési mechanizmushoz használandó protokollok és szabványok

## 5.7. Kommunikációs környezet

## 2. FEJEZET: A daktiloszkópiai adatok cseréje (interfészvezérlési dokumentáció)

1. **Az állományok tartalmának áttekintése**2. **Rekordformátum**3. **1. típusú logikai rekord: állományfejrész**4. **2. típusú logikai rekord: leíró szöveg**5. **4. típusú logikai rekord: nagy felbontású szürkeárnyaltos kép**6. **9. típusú logikai rekord: minuciarekord**7. **13. típusú változó felbontású látenskap-rekord**8. **15. típusú változó felbontású tenyérfotó-kép-rekord**9. **A 2. fejezet függelékei**

## 9.1. ASCII elválasztó kódok

## 9.2. Az alfanumerikus ellenőrző karakter kiszámítása

- 9.3. Karakterkódok
- 9.4. Tranzakcióáttekintés
- 9.5. 1. típusú rekord definíciói
- 9.6. 2. típusú rekord definíciói
- 9.7. Szűrkeskála tömörítési kódok
- 9.8. Levelezési előírások

### 3. FEJEZET: A gépjármű-nyilvántartási adatok cseréje

- 1. **A gépjármű-nyilvántartási adatok automatizált keresésekor használt közös adatkészlet**
  - 1.1. Fogalommeghatározások
  - 1.2. Gépjármű/tulajdonos/üzemben tartó keresése
- 2. **Adatbiztonság**
  - 2.1. Áttekintés
  - 2.2. Az üzenetváltással kapcsolatos biztonsági jellemzők
  - 2.3. Az üzenetváltáshoz nem kapcsolódó biztonsági jellemzők
- 3. **Az adatcsere technikai feltételei**
  - 3.1. Az Eucaris alkalmazás általános ismertetése
  - 3.2. Funkcionális és nem funkcionális követelmények

### 4. FEJEZET: Értékelés

- 1. **A 20. cikk szerinti értékelési eljárás (a 2008/615/IB határozat 25. cikkének (2) bekezdése szerinti határozatok előkészítése)**
  - 1.1. Kérdőív
  - 1.2. Kísérleti adatcsere
  - 1.3. Értékelő látogatás
  - 1.4. Jelentés a Tanács részére
- 2. **A 21. cikk szerinti értékelési eljárás**
  - 2.1. Statisztika és jelentés
  - 2.2. Felülvizsgálat
- 3. **Szakértői értekezletek**

## 1. FEJEZET: DNS-adatok cseréje

## 1. DNS-sel kapcsolatos bűnügyi technikai kérdések, egyezési szabályok és algoritmusok

## 1.1. A DNS-profilok jellemzői

A DNS-profil 24 számpárt tartalmazhat, amelyek az Interpol DNS-eljárásaiban is használt 24 lókuszt alléljait jelölik. E lókuszok neveit az alábbi táblázat tartalmazza:

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

A legfelső sorban szürke színnel jelzett hét lókuszt alkotja jelenleg mind az Európai lókuszt-szabványkészletet (European Standard Set of Loci, ESSOL), mind a lókuszok Interpol-szabványkészletét (Interpol Standard Set of Loci (ISSOL)).

Tartalmi szabályok:

A tagállamok által keresés és összehasonlítás céljából rendelkezésre bocsátott, valamint a keresés és összehasonlítás céljából kiküldött DNS-profiloknak legalább hat teljesen meghatározott <sup>(1)</sup> lókuszt kell magukban foglalniuk, de tartalmazhatnak további lókuszokat vagy szóközöket is, amennyiben azok rendelkezésre állnak. A referencia DNS-profiloknak az európai szabvány részét képező 7 lókuszt közül legalább hatot tartalmazniuk kell. Az egyezések pontosságának javítása érdekében valamennyi allélt tárolni kell az indexált DNS-profilok adatbázisában, és azokat keresés és összehasonlítás céljából használni kell. Valamennyi tagállamnak a lehető leghamarabb át kell vennie bármely, az EU által újonnan elfogadott Európai lókuszt-szabványkészletet (ESSOL).

A vegyes profilok nem engedélyezettek, így az egyes lókuszok allélértékei kizárólag két számból fognak állni, amelyek homozigotizálás esetében egy adott lókuszon meg is egyezhetnek.

A helyettesítő karakterek és a mikrovariánsok az alábbi szabályok szerint kezelendők:

- Az amelogeninen kívül a profilban levő bármely nem numerikus értéket (pl. „o”, „f”, „r”, „na”, „nr” vagy „un”) automatikusan helyettesítő karakterre <sup>(\*)</sup> kell konvertálni az exportálás céljából, és keresést kell indítani az egész adatbázisban.
- A profilban található „0”, „1” vagy „99” numerikus értékeket automatikusan helyettesítő karakterre <sup>(\*)</sup> kell konvertálni az exportálás céljából, és ezeket az adatbázis összes profiljában keresni kell.
- Amennyiben egy lókuszhoz három allél van megadva, az első allélt el kell fogadni, a másik kettőt azonban automatikusan helyettesítő karakterre <sup>(\*)</sup> kell konvertálni az exportálás céljából, és ezeket az adatbázis összes profiljában keresni kell.
- Amennyiben az első vagy a második allélra helyettesítő karaktert adnak meg, a numerikus értéknek a lókuszra vonatkozó mindkét permutációjára keresni kell (pl.: a 12, \* egyezhet 12,14-gyel vagy 9,12-vel is).
- A pentanukleotid (Penta D, Penta E és CD4) mikrovariánsok az alábbiak szerint egyeznek:

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

- A tetranukleotid (a többi lókusz tetranukleotid) mikrovariánsok az alábbiak szerint egyeznek:

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

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

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

<sup>(1)</sup> A „teljesen meghatározott” azt jelenti, hogy a ritka allélértékek kezelését is magában foglalja.

### 1.2. Egyezési szabályok

Két DNS-profil összehasonlítása azon lókuszek alapján történik, amelyekhez mindkét DNS-profilban rendelkezésre áll egy allélpár. Legalább hat teljesen meghatározott lókusznak (az amelogeninen kívül) egyeznie kell mindkét DNS-profilban, mielőtt találati válasz érkezik.

A teljes egyezés (1. minőség) egyezésnek minősül, amennyiben az összehasonlított lókuszeknek a kereső és a lekért DNS-profilban egyaránt megtalálható valamennyi allélértéke megegyezik. A közeli egyezés olyan egyezést jelent, amelynél az összehasonlított allélok közül csupán egynek az értéke tér el a két DNS-profilban (2., 3. és 4. minőség). A közeli egyezés csak akkor fogadható el, ha a két összehasonlított DNS-profilban legalább hat teljesen meghatározott lókuszt egyeznek.

A közeli egyezés okai az alábbiak lehetnek:

- Emberi tévesztés (gépelési hiba) az egyik DNS-profil bevitelénél a keresési kérelemben vagy a DNS-adatbázisban,
- a DNS-profil generálási eljárása során allél-meghatározási vagy allél-lehívási hiba.

### 1.3. Jelentéstételi szabályok

A teljes és a közeli egyezésekről, valamint a találatok hiányáról egyaránt jelentést kell tenni.

Az egyezésről szóló jelentést a kérelmező nemzeti kapcsolattartónak küldik meg, valamint hozzáférhetővé teszi a megkeresett nemzeti kapcsolattartó számára is (annak érdekében, hogy megbecsülhesse a rendelkezésre álló további személyes adatok, valamint a találatnak megfelelő DNS-profillal kapcsolatos egyéb információk iránti, az egyezést követő lehetséges további kérelmek természetét és számát, a 2008/615/IB határozat 5. és 10. cikkével összhangban).

## 2. **Tagállami kódszámok táblázata**

A 2008/615/IB határozattal összhangban a doménnevek és a zárt hálózatban történő prűmi DNS-adatcsere alkalmazásokhoz szükséges egyéb konfigurációs paraméterek meghatározásához az ISO 3166-1 alpha-2 kódot használják.

Az ISO 3166-1 alpha-2 kódok az alábbi, két betűből álló tagállami kódok.

Tagállam	Kód	Tagállam	Kód
Belgium	BE	Luxemburg	LU
Bulgária	BG	Magyarország	HU
Cseh Köztársaság	CZ	Málta	MT
Dánia	DK	Hollandia	NL
Németország	DE	Ausztria	AT
Észtország	EE	Lengyelország	PL
Görögország	EL	Portugália	PT
Spanyolország	ES	Románia	RO
Franciaország	FR	Szlovákia	SK
Írország	IE	Szlovénia	SI
Olaszország	IT	Finnország	FI
Ciprus	CY	Svédország	SE
Lettország	LV	Egyesült Királyság	UK
Litvánia	LT		

### 3. **Funkcionális elemzés**

#### 3.1. A rendszer hozzáférhetősége

A 2008/615/IB határozat 3. cikke szerinti kérelmeknek az egyes kérelmek elküldésének kronológiai sorrendjében kell a céladatbázisba eljutniuk, míg a válaszokat a kérelem megérkezését követő tizenöt percben kell a kérelmező tagállam számára elküldeni.

#### 3.2. Második lépés

Amikor egy tagállam egyezséről szóló jelentést kap, nemzeti kapcsolattartójának feladata a kérdésként benyújtott profilban található értékeknek a válaszként kapott profilban/profilokban található értékekkel való összehasonlítása, a profil bizonyító erejének hitelesítése és ellenőrzése érdekében. A hitelesítés céljából a nemzeti kapcsolattartók közvetlenül is felvehetik egymással a kapcsolatot.

A jogi segítségnyújtási eljárások a két profil közötti egyezés hitelesítését követően kezdődnek meg, az automatizált konzultációs szakasz során elért teljes vagy közeli egyezés alapján.

### 4. **DNS interfészvezérlési dokumentáció**

#### 4.1. Bevezető

##### 4.1.1. Célkitűzések

Ez a fejezet a DNS-profilokban található információknak a tagállamok DNS-adatbázisrendszerei közötti cseréjéhez szükséges előírásokat határozza meg. A fejrészmezőket kifejezetten a primum DNS-adatcserére határozzák meg, az adatrész az Interpol DNS-csere átjárójára meghatározott XML-séma DNS-profil adatrészére alapul.

Az adatcsere az SMTP-protokoll (*Simple Mail Transfer Protocol* – egyszerű levéltovábbítási protokoll) és a legkorszerűbb egyéb technológiák felhasználásával történik, a hálózati szolgáltató által biztosított központi levéltovábbító szerveren keresztül. Az XML-fájlt levéltörzsként továbbítják.

##### 4.1.2. Alkalmazási kör

Az ICD kizárólag az üzenet (levél) tartalmát határozza meg. Minden hálózatspecifikus és levélspecifikus kérdést egységesen határoznak meg, hogy a DNS-adatcsere műszaki alapjai közösek legyenek.

Ez magában foglalja az alábbiakat:

- az üzenet tárgymezőjének formátuma, az üzenet automatizált feldolgozásának lehetővé tétele/engedélyezése érdekében,
- szükséges-e a tartalom rejtjelezése, és amennyiben igen, milyen módszerekkel,
- az üzenetek maximális hossza.

##### 4.1.3. XML-struktúra és -elvek

Az XML-üzenet a következő részekből áll:

- a továbbításra vonatkozó információt tartalmazó fejrész és
- a profilspecifikus információt, valamint magát a profilt tartalmazó adatrész.

A kérelemre és a válaszra egyaránt ugyanazt az XML-sémát kell használni.

A nem azonosított DNS-profilok teljes körű ellenőrzése (a 2008/615/IB határozat 4. cikke) érdekében lehetőség lesz több profil egyetlen üzenetben való elküldésére is. Meg kell határozni az egy üzenetben küldhető profilok maximális számát. A szám a legnagyobb engedélyezett levélmérettől függ, meghatározására a levelezőszerver kiválasztását követően kerül sor.

XML példa:

```
<?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> az adatszerkezetet meg kell ismételni, amennyiben több profilt küldenek (...) egyetlen SMTP-üzenetben,
ami csak a 4. cikkben foglalt esetekben engedélyezett
</datas>]
</PRUEMDNAx>
```

#### 4.2. Az XML szerkezet meghatározása

Az alábbi meghatározások dokumentálási célokat és a jobb olvashatóságot szolgálják, a ténylegesen kötelező információt egy XML-sémafájl tartalmazza (PRUEM DNA.xsd).

##### 4.2.1. PRUEMDNAx s é m a

A s é m a az alábbi mezőket tartalmazza:

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

##### 4.2.2. Fejrészstruktúra tartalma

###### 4.2.2.1. PRUEM fejrész

Ez a struktúra az XML-fájl fejrészét írja le. Az alábbi mezőket tartalmazza:

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

###### 4.2.2.2. PRUEM fejrész

Az üzenetben foglalt adatok típusa, értéke a következő lehet:

Value	Description
R	Request



Value	Description
A	Answer

#### 4.2.2.3. PRUEM fejrészre vonatkozó információk

A tagállamot, valamint az üzenet időpontját/idejét leíró struktúra. Az alábbi mezőket tartalmazza:

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

#### 4.2.3. A PRUEM profil adattartalma

##### 4.2.3.1. PRUEM\_datas

Ez a struktúra az XML profil adatrészét írja le. Az alábbi mezőket tartalmazza:

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

##### 4.2.3.2. PRUEM\_request\_type

Az üzenetben foglalt adatok típusa, értéke a következő lehet:

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

## 4.2.3.3. PRUEM\_hitquality\_type

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

## 4.2.3.4. PRUEM\_data\_type

Az üzenetben foglalt adatok típusa, értéke a következő lehet:

Value	Description
P	Person profile
S	Stain

## 4.2.2.5. PRUEM\_data\_result

Az üzenetben foglalt adatok típusa, értéke a következő lehet:

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

## 4.2.3.6. IPSP\_DNA\_profile

DNS-profil leíró struktúra. Az alábbi mezőket tartalmazza:

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

## 4.2.3.7. IPSP\_DNA\_ISSOL

Az ISSOL lókuszokat (lókuszok Interpol-szabványkészlete) tartalmazó struktúra. Az alábbi mezőket tartalmazza:

Fields	Type	Description
vwa	IPSP_DNA_locus	Locus vwa
th01	IPSP_DNA_locus	Locus th01

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

#### 4.2.3.8. IPSG\_DNA\_additional\_loci

A többi lókuszt tartalmazó struktúra. Az alábbi mezőket tartalmazza:

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

#### 4.2.3.9. IPSG\_DNA\_locus

Lókuszt leíró struktúra. Az alábbi mezőket tartalmazza:

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

## 5. *Alkalmazási, biztonsági és kommunikációs architektúra*

### 5.1. *Áttekintés*

A 2008/615/IB határozat keretében folytatott DNS-adatcsere alkalmazásainak implementációja során közös kommunikációs hálózatot kell használni, amely logikailag zárt lesz a tagállamok között. E közös, a hatékonyabb kérelemküldésre és válaszfogadásra szolgáló kommunikációs infrastruktúra lehetőségeinek a kihasználása

érdekében a DNS- és daktiloszkópiai adatokra irányuló kérelmek kódolt SMTP e-mail üzenetben való továbbítására egy aszinkron mechanizmust fogadnak el. Biztonsági megfontolásból az s/MIME (biztonságos többcélú internetlevelezési bővítvény) mechanizmust mint az SMTP funkció kiterjesztését fogják felhasználni arra, hogy a hálózaton belül egy végpontok közötti biztonságos átjárót építsenek ki.

A tagállamok közötti adatcserét szolgáló kommunikációs hálózat funkcióját a már működő TESTA (a közigazgatási rendszerek közötti transzeurópai telematikai szolgáltatás) tölti be. A TESTA az Európai Bizottság felelősségi körébe tartozik. Figyelembe véve, hogy a nemzeti DNS-adatbázisok és a TESTA jelenlegi nemzeti hozzáférési pontjai esetlegesen a tagállamokban eltérő helyeken található, a TESTA-hoz való hozzáférés kialakítható:

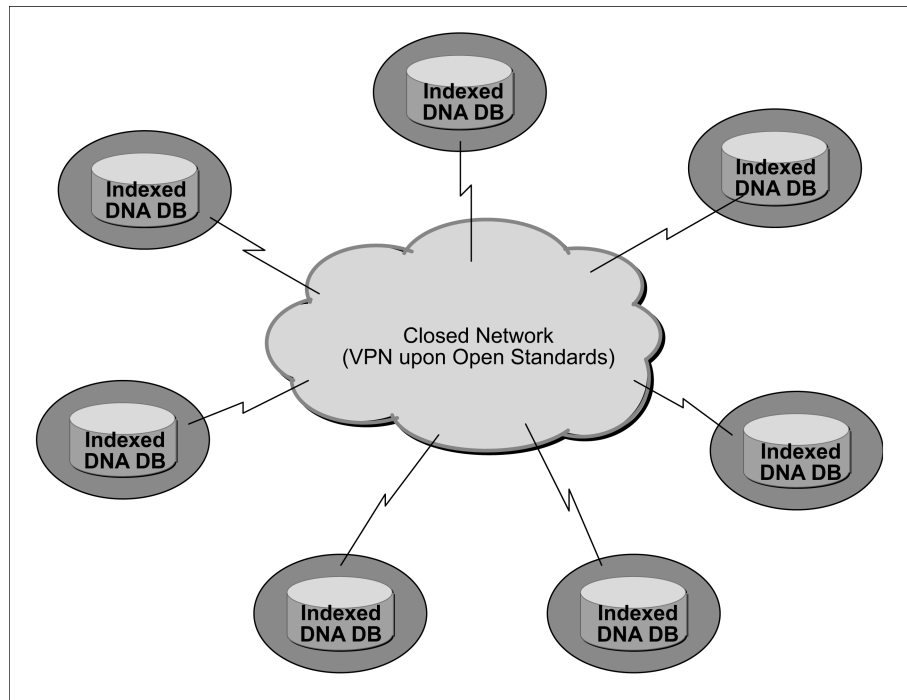
1. a meglévő nemzeti hozzáférési pont felhasználásával, vagy új nemzeti TESTA-hozzáférési pont létrehozásával; vagy
2. egy biztonságos helyi kapcsolat kiépítésével azon hely, ahol a DNS-adatbázis található, és az illetékes nemzeti hatóság azt kezeli, illetve a meglévő nemzeti TESTA-hozzáférési pont helye között.

A 2008/615/IB határozat szerinti alkalmazások végrehajtása során alkalmazott protokollok és szabványok megfelelnek a nyílt szabványoknak és teljesítik a tagállamok nemzeti biztonságpolitikai döntéshozói által előírtakat.

## 5.2. Felső szintű architektúra

A 2008/615/IB határozat alkalmazási körében valamennyi tagállam hozzáférhetővé teszi DNS-adatait a más tagállamokkal való csere és/vagy a más tagállamok általi keresés céljából, az egységesített közös adatformátumnak megfelelően. Az architektúra a bárkitől-bárkinek rendszer kommunikációs modelljére alapul. Nincs sem központi számítógépes szerver, sem pedig központosított adatbázis a DNS-profilok tárolására.

1. ábra: A DNS-adatok cseréjének topológiája



A tagállami helyszínekre vonatkozó nemzeti jogi korlátozások tiszteletben tartásán kívül minden tagállam maga dönthet arról, hogy milyen típusú hardvert és szoftvert alkalmaz a 2008/615/IB határozatban foglalt követelményeknek való megfeleléshez alkalmazandó konfigurációhoz.

## 5.3. Biztonsági előírások és adatvédelem

A biztonsági vonatkozásoknak három szintjét vizsgálták meg és hajtották végre.

### 5.3.1. Adatszint

Az egyes tagállamok által rendelkezésre bocsátott DNS-profilokat a közös adatvédelmi szabványoknak megfelelően kell elkészíteni, úgy hogy a kérelmező tagállam által kézhez kapott válasz elsősorban a találatot (HIT), illetve a találat hiányát (NO HIT) jelezze, találat esetén egy semmilyen személyes információt sem tartalmazó azonosítószámot is feltüntetve. A találatról szóló értesítést követően további vizsgálatokat folytatnak kétoldali szinten, az érintett tagállami helyszínekre vonatkozó meglévő nemzeti jogi és szervezeti szabályoknak megfelelően.

### 5.3.2. Kommunikációs szint

A DNS-profilokra vonatkozó információt tartalmazó üzeneteket (kérelmeket és válaszokat), mielőtt azokat más tagállamok helyszíneire továbbítanák, a nyílt szabványoknak megfelelően a legkorszerűbb módszerekkel, mint például az s/MIME-el rejtjelezzik.

### 5.3.3. Továbbítási szint

A DNS-profilra vonatkozó információt tartalmazó összes rejtjelezett üzenetet nemzetközi szinten egy megbízható hálózati szolgáltató által igazgatott virtuális privát átjárórendszeren keresztül, valamint az ezen átjárórendszerhez kapcsolódó, nemzeti felelősség alá tartozó biztonságos kapcsolatokon keresztül továbbítják a többi tagállam helyszíneire. A virtuális privát átjárórendszernek nincs kapcsolódási pontja a nyilvános internethez.

## 5.4. A titkosítási mechanizmusokhoz használandó protokollok és szabványok: s/MIME és kapcsolódó csomagok

A DNS-profilra vonatkozó információt tartalmazó üzenetek rejtjelezésére az s/MIME nyílt szabványt – mint az SMTP de facto e-mail szabvány kiterjesztését – fogják alkalmazni. Az s/MIME protokoll (V3) lehetővé teszi a levelek aláírását, a biztonsági címkézést és a biztonságos levelezőlistákat; a protokoll a kriptográfiailag védett üzenetekre vonatkozó IETF-szabványra, a kriptográfiai üzenetszintaxisra (*Cryptographic Message Syntax*, CMS) épül. A digitális adatok bármely formájának digitális aláírására, kivonatolására, hitelesítésére és rejtjelezésére szolgál.

Az s/MIME mechanizmus által használt tanúsítványnak meg kell felelnie az X.509 szabványnak. Az egyéb prűmi alkalmazásokkal közös szabvány- és eljáráshasználata biztosítása érdekében az s/MIME rejtjelezési műveletekre vonatkozó, illetve a különböző, kereskedelmi forgalomban kapható termékek (COTS) esetében alkalmazandó eljárási szabályok a következők:

- A művelet sorrendje: először a rejtjelezés, majd az aláírás.
- A szimmetrikus rejtjelezéshez a 256 bites kulcsméretű AES (Advanced Encryption Standard), az aszimmetrikus rejtjelezéshez pedig az 1 024 bites kulcsméretű RSA rejtjelező algoritmust kell alkalmazni.
- Az SHA-1 hash algoritmust kell alkalmazni.

Az s/MIME funkció a modern e-mail szoftvercsomagok közül a legtöbbre, így például az Outlook, a Mozilla Mail, valamint a Netscape Communicator 4.x szoftverbe már be van építve, és a legfőbb e-mail szoftvercsomagokkal kompatibilis.

Mivel az s/MIME könnyen integrálható a nemzeti IT infrastruktúrákba valamennyi tagállami helyszínen, a kommunikációs biztonsági szint implementációjára alkalmas mechanizmusnak bizonyul. A „Proof of Concept” céljának hatékonyabb módon történő elérése, valamint a költségek csökkentése érdekében a DNS-adatok cseréjének prototípezésére viszont a JavaMail API nyílt szabványt választják. A JavaMail API az s/MIME és/vagy az OpenPGP felhasználásával egyszerű rejtjelezést és visszafejtést biztosít. A cél egységes, egyszerűen használható alkalmazásprogramozási interfész (API) biztosítása azon e-mail kliensek számára, akik a két legelterjedtebb e-mail-rejtjelezési formátum valamelyikének felhasználásával kívánják e-mailt küldeni vagy kapni. Ezért a JavaMail API bármely korszerű implementációja megfelel a 2008/615/IB határozat követelményeinek, mint például a Bouncy Castle JCE terméke (Java Cryptographic Extension), amelyet az s/MIME implementációjára fognak használni a DNS-adatok tagállamok közötti cseréjére vonatkozó prototípezés érdekében.

### 5.5. Alkalmazási architektúra

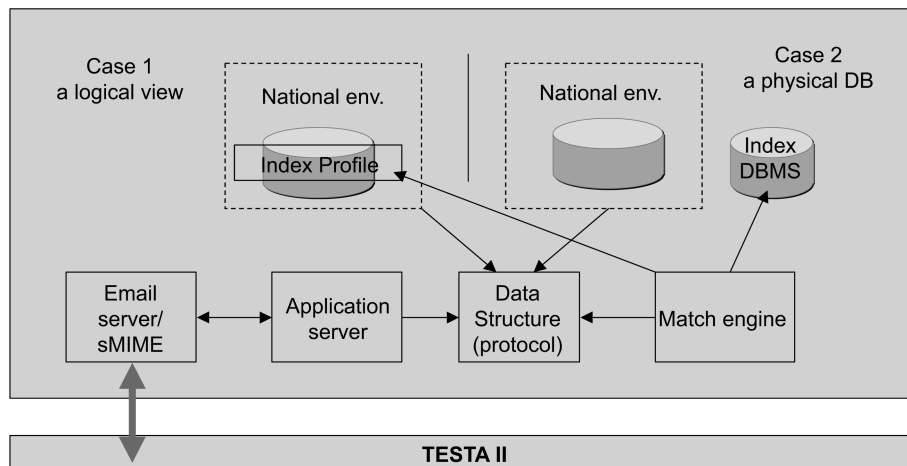
Minden tagállam egy az interfészvezérlési dokumentációval összhangban levő szabványosított DNS-profil adatsomagot bocsát a többi tagállam rendelkezésére. Ez lehetséges az egyes nemzeti adatbázisok logikai nézetének biztosítása vagy fizikai exportált adatbázis (indexált adatbázis) létrehozása által.

A négy fő komponens – az e-mail kiszolgáló/s/MIME, az alkalmazáskiszolgáló, az adatlekérdezésre és -bevitelre, a bejövő és kimenő üzenetek nyilvántartására szolgáló adatstruktúra-terület, továbbá az összehasonlító motor – termékfüggetlen módon implementálja a teljes alkalmazási logikát.

Annak biztosítása érdekében, hogy a tagállamok könnyen integrálhassák a komponenseket saját nemzeti rendszereikbe, a meghatározott közös funkcionalitást a tagállamok által nemzeti IT politikájuktól és szabályaiktól függetlenül választható nyílt forráskódú komponensek útján érték el. A 2008/615/IB határozat hatálya alá tartozó DNS-profilokat tartalmazó indexált adatbázisokhoz való hozzáférés megszerzéséhez implementálandó jellemzők függetlensége miatt minden tagállam szabadon választhatja meg hardver- és szoftverplatformját, beleértve az adatbázis- és operációs rendszereket is.

A meglévő közös hálózatban kifejlesztették, és sikeresen tesztelték a DNS-adatok cseréjének prototípusát. Az 1.0 verzió produktív környezetben való alkalmazása megkezdődött, és azt a napi műveletekben használják. A tagállamok használhatják a közösen kifejlesztett terméket, de kifejleszthetik saját termékeiket is. A közös termékkomponenseket az IT, valamint a bűnügyi technikai és/vagy funkcionális rendőrségi követelmények változásának megfelelően fogják karbantartani, teszte szabni és továbbfejleszteni.

2. ábra: Alkalmazás-topológiai áttekintés



### 5.6. Az alkalmazási architektúrához használandó protokollok és szabványok

#### 5.6.1. XML

A DNS-adatok cseréje teljes mértékben az XML-sémát – mint az SMTP e-mail üzenetek csatolmányát – adatait ki. A Kiterjeszhető Leíró Nyelv (XML) a W3C által ajánlott általános célú leíró nyelv, amely speciális célú leíró nyelvek létrehozására szolgál, és amely számos különböző adattípus leírására képes. A valamennyi állam közötti cserére alkalmas DNS-profil leírása XML és XML-séma alkalmazásával történt az interfészvezérlési dokumentumban.

#### 5.6.2. ODBC

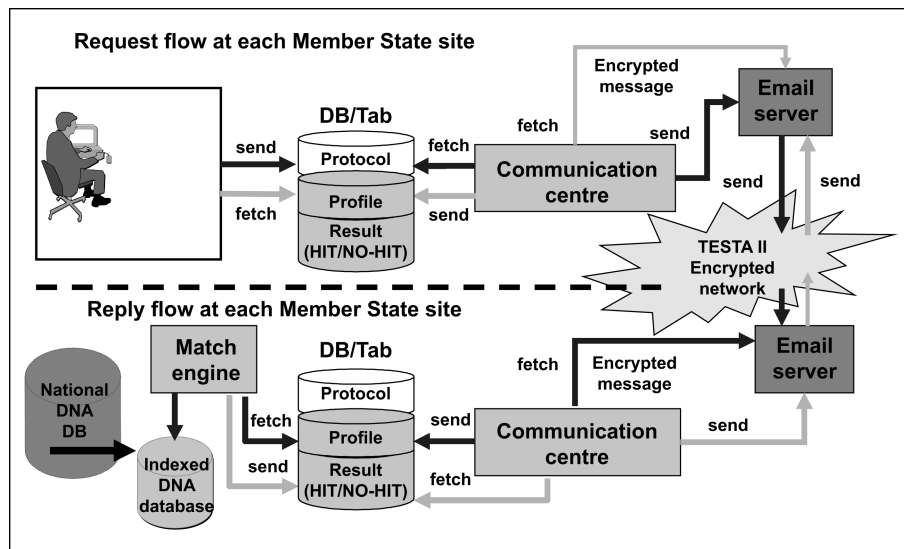
A nyílt adatbázis-kapcsolat (ODBC) szabványos szoftveres API metódust kínál az adatbázis-kezelő rendszerekhez való hozzáféréshez, és függetlenséget biztosít a programozási nyelvektől, valamint az adatbázis- és operatív rendszerektől. Az ODBC-nek ugyanakkor vannak hátrányai is. A nagy számú ügyfélgép kezelése különböző eszközmeghajtókat és dinamikusan kapcsolódó könyvtárakat (DLL) jelenthet. Ez az összetettség rendszerfelületi többletmunkát eredményezhet.

## 5.6.3. JDBC

A JAVA adatbázis-kapcsolat (JDBC) egy API a Java programozási nyelvhez, amely azt határozza meg, hogy egy ügyfél hogyan férhet hozzá egy adatbázishoz. Az ODBC-től eltérően a JDBC esetében nincs szükség bizonyos helyi DLL-ek használatára a munkaállomáson.

A DNS-profilokra vonatkozó kérelmeknek és válaszoknak az egyes tagállami helyszíneken való feldolgozása üzleti logikáját az alábbi ábra mutatja be. A kérelem- és válaszáramok egyaránt egy olyan neutrális adatterülettel állnak kölcsönhatásban, amely különböző, közös adatszerkezetű adatállományokat tartalmaz.

3. ábra: Áttekintés: Az alkalmazás munkafolyamata az egyes tagállami helyszíneken



## 5.7. Kommunikációs környezet

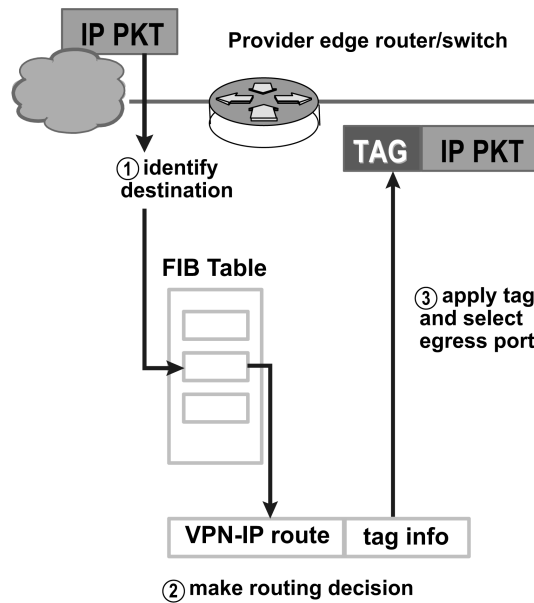
## 5.7.1. Közös kommunikációs hálózat: TESTA és az arra épülő infrastruktúra

A DNS-adatcsere alkalmazás az e-mailt mint aszinkron mechanizmust használja a tagállamok közötti kérelemküldésre és válaszfogadásra. Mivel minden tagállamnak van legalább egy nemzeti hozzáférési pontja a TESTA hálózathoz, a DNS-adatok cseréjére a TESTA hálózaton keresztül kerül sor. A TESTA számos, hozzáadott értéket képviselő szolgáltatást is nyújt e-mail-továbbító rendszerén keresztül. A TESTA-specifikus elektronikus postafiókok hostingja mellett az infrastruktúra levélelosztó listákat és hálózati forgalomirányító (routing) szabályokat is tud alkalmazni. Ez lehetővé teszi, hogy a TESTA az EU-ban létező doménekhez kapcsolódó közigazgatási szervekhez címzett üzenetek elszámolóháza legyen. Vírusellenőrző rendszerek is telepíthetők.

A TESTA e-mail továbbítója a TESTA központi alkalmazási egységeiben elhelyezett, tűzfalal védett, nagy üzembiztonságú hardverplatformra épül. A TESTA DNS-szolgáltatása az erőforrás-azonosítókat IP-címekké oldja fel, továbbá a felhasználó és az alkalmazások előtt elrejtja a címinformációkat.

## 5.7.2. Biztonsági megfontolások

A virtuális magánhálózat (VPN) koncepcióját a TESTA keretében hozták létre. Az ennek a virtuális magánhálózatnak a kiépítésére használt címkekapcsolási technológia fogja majd az Internet Műszaki Testület (IETF) által kifejlesztett többprotokollos címkekapcsolás (MPLS) szabványát támogatni.



Az MPLS olyan IETF szabványtechnológia, amely felgyorsítja a hálózati adatáramlást azáltal, hogy kihagyja a köztes hálózati forgalomirányítók (routerek) általi csomagelvezést. Mindez a gerincvezeték határroute-ri által a továbbítási adatbázisban tárolt információk alapján a csomaghoz csatolt ügynevezett címkek alapján történik. A címkek a virtuális magánhálózatok létrehozására is szolgálnak.

Az MPLS a 3-as rétegű hálózati forgalomirányítás (routing) és a 2-es rétegű kapcsolás előnyeit kombinálja. Mivel az IP-címeket a gerincvezetéken való átmenet során nem értékelik, az MPLS az IP-címzések tekintetében nem szab semmilyen korlátot.

Ezenfelül a TESTA-n keresztül küldött e-mail üzeneteket s/MIME alapú rejtjelezési mechanizmus is védi. A kulcs ismeretének és a megfelelő tanúsítvány birtokának hiányában senki sem tudja a hálózaton keresztül küldött üzeneteket megfejteni.

### 5.7.3. A kommunikációs hálózatban használandó protokollok és szabványok

#### 5.7.3.1. SMTP

Az egyszerű levéltovábbítási protokoll (SMTP-protokoll) az Interneten keresztüli e-mail továbbítás de facto szabványa. Az SMTP egy viszonylag egyszerű, szövegalapú protokoll, amelyben meghatározzák az üzenet egy vagy több címzettjét, majd az üzenet szövegét továbbítják. Az SMTP az IETF előírásai alapján a 25-ös TCP portot használja. Egy adott domén névre vonatkozóan az SMTP szerver meghatározására az MX (Mail eXchange) DNS (Domain Name Systems) rekordot használják.

Mivel ez a protokoll tisztán ASCII szövegalapúnak indult, nem tudta jól kezelni a bináris állományokat. A MIME-hez hasonló szabványokat a bináris állományoknak az SMTP-n keresztül való továbbítás céljából történő kódolására fejlesztették ki. Ma a legtöbb SMTP szerver támogatja a 8BITMIME és az s/MIME kiterjesztést, lehetővé téve így, hogy a bináris állományokat csaknem ugyanolyan egyszerűen továbbítsák, mint az egyszerű szöveget. Az s/MIME műveletekre vonatkozó feldolgozási szabályokat az s/MIME-ről szóló szakasz írja le (lásd az 5.4. pontot).

Az SMTP kézbesítő rendszer, amely nem engedi, hogy bárki üzenetet hívjon le egy távoli szerverről kérésre. Ehhez az e-mail kliensnek POP3-at vagy IMAP-ot kell használnia. A DNS-adatok cseréjének végrehajtása keretében a POP3 protokoll alkalmazásáról született döntés.

#### 5.7.3.2. POP

A helyi e-mail kliensek az elektronikus levelek távoli szerverről TCP/IP kapcsolaton keresztül való letöltéséhez a Post Office Protocol 3. változatát (POP3) használják, amely egy alkalmazás szintű internetes szabvány protokoll. Az SMTP protokoll SMTP küldési profiljának alkalmazásával az e-mail kliensek az interneten vagy egy egyesített hálózaton keresztül üzeneteket küldenek. A MIME az e-mail csatolmányaihoz és nem ASCII-szövegrészeihez használt szabvány. Bár sem a POP3, sem az SMTP nem írja elő a MIME formátumú leveleket, az interneten keresztül küldött e-mailek alapvetően MIME formátumúak, ezért a POP-klienseknek érteniük és használniuk kell a MIME-et is. Következésképpen a 2008/615/IB határozat egész kommunikációs környezete magában fogja foglalni a POP komponenseit.



## 5.7.4. Hálózati címek kiosztása

## Operatív környezet

Az Európai IP-regisztrációs Szervezet (RIPE) a TESTA-nak jelenleg saját C osztályú alhálózati blokkot osztott ki. Szükség esetén a jövőben további címblokkok kiosztása is elképzelhető a TESTA számára. Az IP-címek tagállamok számára történő kiosztása Európában földrajzi alapon történik. A tagállamok között a 2008/615/IB határozat keretében megvalósuló adatcsere egy európai szintű, logikailag zárt IP-hálózaton keresztül történik.

## Tesztkörnyezet

Annak érdekében, hogy a kapcsolódó összes tagállamban akadálymentes környezetben lehessen a mindennapi műveleteket elvégezni, a műveletekbe való bekapcsolódásuk előkészítése érdekében a zárt hálózaton belül tesztkörnyezetet kell kialakítani az új tagállamok számára. Összeállítottak egy IP-címeket, hálózati beállításokat, e-mail doméneket és alkalmazásfelhasználói fiókokat magában foglaló paraméterlistát; ezeket a megfelelő tagállami helyszíneken létre kell hozni. Ezenfelül tesztcélokra pseudo DNS-profilokat is létrehoztak.

## 5.7.5. Konfigurációs paraméterek

Létrejött az eu-admin.net domént használó biztonságos e-mail rendszer. Ez a domén és a hozzá kapcsolódó címek nem érhetők el a nem az európai szintű TESTA doménen levő helyről, mivel a neveket kizárólag a TESTA internet elől árnyékolt központi DNS-kiszolgálója ismeri.

Ezen TESTA-webcímekek (gazdanevek) IP-címekhez való hozzárendelését a TESTA DNS-szolgáltatása végzi. Ez a központi TESTA DNS-kiszolgáló valamennyi helyi doménre új mailt jegyez be, amely a helyi TESTA-doménekre küldött leveleket továbbítja a központi TESTA-levéltovábbító felé. Ez a központi TESTA-levéltovábbító továbbítja majd az e-maileket a konkrét helyi doménnevű e-mail kiszolgálónak, a helyi doménnevű e-mail címek felhasználásával. Az e-mailek ilyen módon történő továbbításával a levelekben foglalt kritikus információ kizárólag az európai szintű zárt hálózati infrastruktúrán halad keresztül, a nem biztonságos interneten keresztül nem.

A tagállami helyszíneken aldoméneket (*félkövér, dőlt*) kell létrehozni, az alábbi szintaxis szerint:

„*alkalmazás-típus.pruem.tagállam-kód.eu-admin.net*”, ahol:

a „*tagállam-kód*”: a két betűből álló tagállami kódok egyikének értéke (pl. AT, BE, stb.),

„*alkalmazás-típus*”: az alábbi értékek egyike: DNA és FP.

A fenti szintaxis alkalmazásának eredményeként létrejövő tagállami aldoméneket az alábbi táblázat foglalja össze:

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

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

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

## 2. FEJEZET: A daktiloszkópiai adatok cseréje (interfészvezérlési dokumentáció)

Az alábbi, dokumentumokra vonatkozó interfészvezérlési dokumentáció célja a daktiloszkópiai adatoknak a tagállamok automatizált ujjnyomat-azonosító rendszerei (AFIS) közötti cseréjére vonatkozó követelmények meghatározása. Ennek alapja az ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b) Interpol általi implementációja.

E változat tartalmazza a kép- és minucia-alapú daktiloszkópiai eljáráshoz szükséges 1., 2., 4., 9., 13. és 15. típusú logikai rekordok valamennyi alapdefinícióját.

### 1. Az állományok tartalmának áttekintése

Egy daktiloszkópiai állomány több logikai rekordból áll. Az eredeti ANSI/NIST-ITL 1-2000 szabvány tizenhatféle rekordtípust határoz meg. A rekordokat, valamint a rekordokon belül a mezőket és almezőket megfelelő ASCII elválasztó karakterek választják el egymástól.

A származási és a rendeltetési szervezet közötti információcserében csupán 6 rekordtípust alkalmaznak:

- 1. típus → A tranzakcióra vonatkozó információk
- 2. típus → A személyekre/ügyre vonatkozó alfanumerikus adatok
- 4. típus → Nagy felbontású szürkeárnyalatos daktiloszkópiai kép
- 9. típus → Minucia rekord
- 13. típus → Változó felbontású látenskap-rekord
- 15. típus → Változó felbontású tenyérynymatkép-rekord

#### 1.1. 1. típus – Állományfejlesztés

E rekord hálózati forgalomirányító (routing) információkat és az állomány többi részének a struktúráját leíró információkat tartalmaz. E rekordtípus határozza meg továbbá a tranzakciók típusait, amelyek az alábbi nagy kategóriákba sorolhatók:

#### 1.2. 2. típus – Leíró szöveg

E rekord a küldő és fogadó szervezetek számára jelentőséggel bíró szöveges információkat tartalmaz.

#### 1.3. 4. típus – Nagy felbontású szürkeárnyalatos kép

E rekord 500 pixel/hüvelyk mintavételezésű, nagy felbontású szürkeárnyalatos (nyolc bites) daktiloszkópiai képek cseréjére szolgál. A daktiloszkópiai képek tömörítése a WSQ algoritmussal történik, és legfeljebb 15:1 arányú lehet. Tilos az ettől eltérő tömörítési algoritmusok vagy tömörítés nélküli képek használata.

#### 1.4. 9. típus – Minucia rekord

A 9. típusú rekordok a fodorszálak jellemzőinek vagy a minucia-adatoknak a cseréjére szolgálnak. Céljuk egyrészt az AFIS kódolási eljárásai felesleges megkettőzésének elkerülése, másrészt pedig azon AFIS-kódok továbbításának lehetővé tétele, amelyek a hozzájuk tartozó képeknél kevesebb adatot tartalmaznak.

#### 1.5. 13. típus – Változó felbontású látens kép-rekord

E rekord a változó felbontású látens ujjnyomat- és látens tenyérnyomat-képeknek az alfanumerikus szöveges információkkal együtt történő cseréjére szolgál. A képek szkennelési felbontása 500 pixel/hüvelyk 256 szűrkeségi szinttel. Amennyiben a látens kép minősége megfelelő, WSQ algoritmussal kell tömöríteni. Kétoldalú megállapodás alapján a képek felbontása szükség esetén nagyobb is lehet, mint 500 pixel/hüvelyk és 256 szűrkeségi szint. Ez esetben erősen ajánlott a JPEG 2000 használata (lásd a 7. függelékét).

#### 1.6. Változó felbontású tenyérnyomatkép-rekord

A 15. típusú címkézettmező-képrekordok a változó felbontású tenyérnyomatképeknek az alfanumerikus szöveges információkkal együtt történő cseréjére szolgálnak. A képek szkennelési felbontása 500 pixel/hüvelyk 256 szűrkeségi szinttel. Az adatok mennyiségének a lehető legkisebbre csökkentése érdekében valamennyi tenyérnyomatképet a WSQ algoritmussal kell tömöríteni. Kétoldalú megállapodás alapján a képek felbontása szükség esetén nagyobb is lehet, mint 500 pixel/hüvelyk és 256 szűrkeségi szint. Ez esetben erősen ajánlott a JPEG 2000 használata (lásd a 7. függelékét).

## 2. **Rekordformátum**

Egy tranzakciós állomány egy vagy több logikai rekordból áll. Az állományban szereplő valamennyi logikai rekordhoz több, az adott rekordtípusnak megfelelő információs mező tartozik. Minden információs mező egy vagy több alapvető egyértékű adatelemet tartalmazhat. Ezen elemek együttesen a mezőben szereplő adatok különböző aspektusainak bemutatására szolgálnak. Az információs mezők egy vagy több, csoportba foglalt és a mezőn belül többször ismételt adatelemből is állhatnak. Az adatelemek ezen csoportja az almező. Az információs mezők tehát az adatelemek által alkotott egy vagy több almezőből is állhatnak.

### 2.1. *Adatelválasztók*

A címkézett mező típusú logikai rekordokban az adatok határait a négy ASCII adatelválasztó használatával kell jelölni. A körülhatárolt adatok lehetnek egy mezőn vagy almezőn belüli adatelemek, egy logikai rekordon belüli mezők vagy a többször ismétlődő almezők. Ezen adatelválasztók az ANSI X3.4 szabványban vannak meghatározva. E karakterek az adatok logikai alapon történő elválasztására és minősítésére szolgálnak. Hierarchikus összefüggésben az „FS” állományelválasztó karakter a legátfogóbb, ezt követi a „GS” csoportelválasztó, az „RS” rekordelválasztó és végül az „US” egységelválasztó karakter. Ezen ASCII-elválasztók listája és az e szabvány szerinti használatuk leírása az 1. táblázatban található.

Funkcionális értelemben az adatelválasztók azt jelzik, hogy milyen típusú adat következik. Az „US” karakter a mezőn vagy almezőn belüli egyes adatelemeket választja el egymástól. Azt jelzi, hogy a következő adatelem az adott mező vagy almező egy adateleme. Az egy mezőn belüli több almezőt elválasztó „RS” karakter az ismétlődő adatelem(ek) következő csoportjának a kezdetét jelzi. Az információs mezők közötti „GS” elválasztó karakter egy új mező kezdetét jelzi, és megelőzi a következő mező azonosítószámát. A fentiekhez hasonlóan az „FS” karakter egy új logikai rekord kezdetét jelzi.

A négy karakternek csak akkor van értelme, ha az ASCII szövegrekordok mezőiben az adatelemek elválasztására alkalmazzák azokat. A bináris képrekordokban és bináris mezőkben előforduló ilyen karakterekhez nem társul konkrét jelentés – azok csupán részei a kicserélt adatoknak.

Általában nem fordulhatnak elő üres mezők vagy adatelemek, így csak egy elválasztó karakter állhat két adatelem között. E szabály alól azok az esetek képeznek kivételt, amikor egy tranzakciónál nem állnak rendelkezésre, hiányoznak, vagy nem kötelezők egyes mezők vagy adatelemek adatai, és a tranzakció feldolgozása nem függ ezen adatok meglététől. Ilyen esetben több elválasztó karakter állhat egymás mellett, és nem kell helykitöltő adatokkal feltölteni az elválasztó karakterek közötti helyet.

Egy három adatelemből álló mező meghatározásakor az alábbiakat kell alkalmazni. Ha a második adatelem adatai hiányoznak, akkor két „US” adatelválasztó karakter áll egymás mellett az első és a harmadik adatelem között. Ha a második és harmadik adatelem is hiányzik, akkor három elválasztó karaktert kell használni – két „US” karaktert, valamint a mezőt vagy mezőt lezáró elválasztó karaktert. Általánosságban, ha egy mezőben vagy almezőben egy vagy több kötelező vagy nem kötelező adatelem nem áll rendelkezésre, akkor be kell illeszteni a megfelelő számú elválasztó karaktert.

Lehetőség van a négy lehetséges elválasztó karakter közül kettő vagy több egymás melletti kombinációjának alkalmazására. Amennyiben egyes adatelemek, almezők vagy mezők adatai hiányoznak vagy nem hozzáférhetők, az elválasztó karakterek számának a szükséges adatelemek, almezők vagy mezők számánál eggyel kisebbnek kell lennie.

1. táblázat: A használható elválasztók

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. Rekordszerkezet

A címkézett mező típusú logikai rekordokban minden adatelemet meg kell számozni e szabványnak megfelelően. Minden mezőnek tartalmaznia kell a logikai rekord típusának számát, amelyet egy pont „.” követ, a mező számát, amelyet kettőspont „.” követ, majd a mezőnek megfelelő információt. A címkézett mező száma bármilyen egytől kilencig terjedő szám lehet, amelyet a pont „.” és a kettőspont „.” fog közre. A mezőszám előjel nélküli egész számként értelmezendő. Ebből következően a „2.123.” mezőszám megegyezik a „2.000000123.” mezőszámmal, és ugyanolyan módon értelmezendő.

E dokumentumban illusztrációképpen egy háromjegyű számot fogunk használni az ismertetett címkézett mező típusú logikai rekordok mezőinek számozására. A mezőszámok formátuma „TT.xxx.” lesz, ahol „TT” a rekordtípus egy vagy két karakterből álló száma, amelyet egy pont követ. A következő három karakter az adott mezőszám, amelyet kettőspont követ. A kettőspont után leíró ASCII-adatok vagy képadatok állnak.

Az 1. és 2. típusú logikai rekordok csak ASCII szöveges adatmezőket tartalmaznak. E rekordtípusok esetében az első ASCII-mező a rekord teljes hosszát (beleértve a mezőszámokat, kettőspontokat és elválasztó karaktereket) tartalmazza. Az ASCII-adatok utolsó bájtyát az „FS” ASCII szerinti állományelválasztó (a logikai rekord vagy tranzakció végét jelző) vezérlőkarakter követi, amely beleszámít a rekord hosszába.

A címkézett mezővel szemben a 4. típusú rekord kizárólag bináris adatokat tartalmaz rendezett, rögzített hosszú bináris mezők formájában. Minden rekord első négybájtos bináris mezője tartalmazza a rekord teljes hosszát. E bináris rekordban nem szerepel sem a rekordszám a ponttal, sem a mező azonosítószáma az azt követő kettősponttal. Továbbá, mivel e rekordban valamennyi mező rögzített vagy meghatározott hosszú, a fenti négy elválasztó karaktert („US”, „RS”, „GS” vagy „FS”) minden esetben kizárólag bináris adatként kell értelmezni. A bináris rekordban az „FS” karakter nem használható rekordelválasztó vagy tranzakciót záró karakterként.

## 3. 1. típusú logikai rekord: állományfejrész

E rekord az állomány struktúráját, az állomány típusát és egyéb fontos információkat tartalmaz. Az 1. típusú mezőkben alkalmazott karakterkészlet kizárólag az információcsere céljára használatos 7-bites ANSI-kódot tartalmazhatja.

### 3.1. Az 1. típusú logikai rekord mezői

#### 3.1.1. 1.001 mező: A logikai rekord hossza (Logical Record Length – LEN)

E mező tartalmazza a teljes 1. típusú logikai rekordban található bájtok számát. A mező az „1001:” karakterekkel kezdődik, ezt követi a rekord teljes hossza, beleértve minden mező minden karakterét és az adatelválasztókat.

### 3.1.2. 1.002 mező: Verziószám (Version Number – VER)

Annak érdekében, hogy a felhasználók tisztában legyenek az ANSI/NIST-szabvány használt verziójával, ez a négybájtos mező meghatározza, hogy az állományt létrehozó szoftver vagy rendszer a szabvány mely verziószerű változatát alkalmazza. Az első két bájttal határozza meg a fő verziószámot, a második kettő pedig a másodlagos változatszámot. Az eredeti, 1986-os szabvány lenne például az első verzió és ezért ez a „0100” számot kapná, míg a jelenlegi ANSI/NIST-ITL 1-2000 szabvány a „0300”.

### 3.1.3. 1.003 mező: Az állomány tartalma (File Content – CNT)

E mező tartalmazza az állomány valamennyi rekordjának rekordtípusok szerinti felsorolását, valamint a rekordok sorrendjét a logikai állományban. Egy vagy több almezőből áll, amelyek mindegyike két olyan adatelemet tartalmaz, amely egy, az adott állományban található logikai rekordot ír le. Az almezők a rekordok bejegyzésével és továbbításával megegyező sorrendben kerülnek bevitelre.

Az első almező első adateleme „1”, amely az 1. típusú rekordra utal. Ezt egy második adatelem követi, amely az állományban szereplő többi rekord számát tartalmazza. E szám megegyezik továbbá az 1.003 mező fennmaradó almezőinek számával.

A fennmaradó almezők mindegyike az állomány egyik rekordjához kapcsolódik, és az almezők sorrendje megegyezik a rekordok sorrendjével. Mindegyik almező két adatelemet tartalmaz. Az első a rekord típusának meghatározására szolgál. A második a rekord IDC-je. A két adatelemet az „US” karakter választja el egymástól.

### 3.1.4. 1.004 mező: A tranzakció típusa (Type of Transaction – TOT)

E mező egy három betűből álló, a tranzakció típusát meghatározó mnemonikus kódot tartalmaz. E kódok eltérhetnek az ANSI/NIST-szabvány más alkalmazásaiban használt kódoktól.

CPS: Mintanyomathoz mintanyomat bűnügy kapcsán történő keresése (Criminal Print-to-Print Search). E tranzakció egy bűncselekménnyel kapcsolatos rekordnak egy ujj- és tenyérynymatokat tartalmazó adatbázisban való keresésére irányuló kérelem. Az állománynak WSQ-tömörítésű képek formájában tartalmaznia kell a személy ujj- és tenyérynymatait.

Amennyiben nincs találat (No-HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord.

Amennyiben van találat (HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord,
- 1–14 4. típusú rekord.

A CPS TOT összefoglalása az A.6.1. táblázatban (6. függelék) található.

PMS: Mintanyomathoz nyom keresése (Print-to-Latent Search). E tranzakció az ujj- és tenyérynymatokat azonosítatlan látens képeket tartalmazó adatbázisban történő keresésére szolgál. Az eredmény tartalmazza, hogy a rendeltetés szerinti AFIS-ben végzett keresés ad-e találatot (Hit/No-Hit). Ha több azonosítatlan látens kép létezik, az eredmény több SRE tranzakció lesz, ahol minden tranzakcióhoz egy látens kép kapcsolódik. Az állománynak WSQ-tömörítésű képek formájában tartalmaznia kell a személy ujj- és tenyérynymatait.

Amennyiben nincs találat (No-HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord.

Amennyiben van találat (HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord,
- 1 13. típusú rekord.

A PMS TOT összefoglalása az A.6.1. táblázatban (6. függelék) található.

MPS: Nyomhoz mintanyomat keresése (Latent-to-Print Search). E tranzakció látens képeknek az ujj- és tenyérynymatokat tartalmazó adatbázisban történő keresésére szolgál. Az állománynak tartalmaznia kell a látens minuciákra vonatkozó információkat és a (WSQ-tömörítésű) képet.

Amennyiben nincs találat (No-HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord.

Amennyiben van találat (HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord,
- 1 4. típusú vagy 15. típusú rekord.

Az MPS TOT összefoglalása az A.6.4. táblázatban (6. függelék) található.

MMS: Nyomhoz nyom keresése (Latent-to-Latent Search). E tranzakciónál az állomány egy látens képet tartalmaz, amelyet azonosítatlan látens nyomatokat tartalmazó adatbázisban kell keresni a különböző bűncselekmények elkövetésének helyei közötti kapcsolatok megállapítása céljából. Az állománynak tartalmaznia kell a látens minuciákra vonatkozó információkat és a (WSQ-tömörítésű) képet.

Amennyiben nincs találat (No-HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord.

Amennyiben van találat (HIT), a keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord,
- 1 13. típusú rekord.

Az MMS TOT összefoglalása az A.6.4. táblázatban (6. függelék) található.

SRE: A rendeltetési szervezet ezt a tranzakciót adja válaszul a daktiloszkópiai kérelmekre. Az eredmény tartalmazza, hogy a rendeltetés szerinti AFIS-ben végzett keresés ad-e találatot (Hit/No-Hit). Ha több potenciális találat van, az eredmény több SRE-tranzakció lesz, ahol minden tranzakcióhoz egy potenciális találat kapcsolódik.

Az SRE TOT összefoglalása az A.6.2. táblázatban (6. függelék) található.

ERR: A rendeltetés szerinti AFIS ezt a tranzakciót adja válaszul, ha hiba történt a tranzakció során. Tartalmaz egy, a talált hibát azonosító üzenetmezőt (ERM). A keresés eredményei az alábbi logikai rekordok lesznek:

- 1 1. típusú rekord,
- 1 2. típusú rekord.

Az ERR TOT összefoglalása az A.6.3. táblázatban (6. függelék) található.

2. táblázat: A tranzakciókban alkalmazható kódok

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	—	—	—	—

Jelmagyarázat:

- M = Kötelező  
M\* = A két rekordtípusból csak egy alkalmazható  
O = Nem kötelező  
C = Akkor alkalmazandó, ha rendelkezésre állnak az adatok  
– = Nem engedélyezett  
1\* = A kiváltandó rendszerektől (legacy system) függően alkalmazandó

3.1.5. 1.005 mező: A tranzakció dátuma (Date of Transaction – DAT)

E mező jelöli a tranzakció kezdeményezésének dátumát, és formátumának meg kell felelnie az ISO-szabvány szerinti jelölésnek: YYYYMMDD

ahol YYYY az év, MM a hónap és DD a hónap napja. Az egyjegyű számok elé nullát kell tenni. „19931004” például 1993. október 4-ét jelenti.

3.1.6. 1.006 mező: Prioritás (Priority – PRY)

Ez a nem kötelező mező határozza meg a kérelem prioritását egy 1-től 9-ig terjedő skálán. „1” jelenti a legnagyobb prioritást, „9” a legkisebbet. Az „1” prioritású tranzakciók haladéktalanul végrehajtandók.

3.1.7. 1.007 mező: A rendeltetési szervezet azonosítója (Destination Agency Identifier – DAI)

E mező határozza meg a tranzakció rendeltetési szervezetét.

Két adatelemből áll, és formátuma a következő: CC/szervezet.

Az első adatelem tartalmazza az ISO 3166 szerinti országcódot (CC), amely két alfanumerikus karakter hosszú. A második elem – a szervezet – szabad szövegű meghatározás legfeljebb 32 alfanumerikus karakterig.

3.1.8. 1.008 mező: A származási szervezet azonosítója (Originating Agency Identifier – ORI)

E mező határozza meg az állomány kibocsátóját, és formátuma megegyezik a DAI (1.007 mező) formátumával.

3.1.9. 1.009 mező: Tranzakció nyilvántartási szám (Transaction Control Number – TCN)

Ez egy hivatkozási célokra szolgáló nyilvántartási szám. A számítógép generálja, és formátuma a következő: YYSSSSSSSA

ahol YY a tranzakció éve, SSSSSSSS egy nyolcjegyű sorozatszám, az A pedig egy, a 2. függelékben meghatározott eljárás szerint generált ellenőrző karakter.

Ha a TCN nem áll rendelkezésre, a mező YYSSSSSSSS részét nullákkal kell feltölteni, az ellenőrző karakter generálása pedig a fentiek szerint történik.

3.1.10. 1.010 mező: A tranzakciós kérelem nyilvántartási száma (Transaction Control Response – TCR)

A kiküldött kérelmekre adott válaszokban ez a nem kötelező mező a kérelem üzenetének tranzakció nyilvántartási számát tartalmazza. Formátuma ebből következően megegyezik a TCN (1.009 mező) formátumával.

3.1.11. 1.011 mező: Natív szkennelési felbontás (Native Scanning Resolution – NSR)

E mező a rendszernek a tranzakció kibocsátója által támogatott szokásos szkennelési felbontását tartalmazza. A felbontás meghatározásának formátuma két numerikus karakter, amelyet a tizedesjel követ, majd két további számjegy.



A 2008/615/IB határozat szerinti valamennyi tranzakció esetében a mintavételi arány 500 pixel/hüvelyk vagy 19,68 pixel/mm.

3.1.12. 1.012 mező: Névleges adatátviteli felbontás (Nominal Transmitting Resolution – NTR)

Ez az ötbájtos mező határozza meg a továbbított képek névleges adatátviteli felbontását. A felbontást pixel/mm-ben kell megadni, az NSR-rel (1.011 mező) megegyező formátumban.

3.1.13. 1.013 mező: Doménnév (Domain name – DOM)

Ez a kötelező mező határozza meg a doménnevet a 2. típusú felhasználói logikai rekord implementációjához. Két adatelemből áll, értéke „INT-I{US}4.22{GS}”.

3.1.14. 1.014 mező: Greenwichi középidő (Greenwich mean time – GMT)

Ez a kötelező mező mechanizmust biztosít a dátumnak és az időpontnak az univerzális greenwichi középidő (GMT) egységeiben való kifejezésére. Használata esetén a GMT mező az univerzális időt tartalmazza, ami kiegészíti az 1.005 (DAT) mezőben foglalt helyi időt. A GMT mező használata kiküszöböli a helyi idők közötti eltéréseket, ami akkor tapasztalható, ha a tranzakció és az ahhoz kapcsolódó válasz két olyan hely között kerül továbbításra, amelyeket több időzóna választ el egymástól. A GMT univerzális dátumot tartalmaz, valamint időzónáktól független, 24-órás formátumú órajelzést. A mező formátuma a „CCYYMMDDHHMMSSZ” 15 elemből álló karakterlánc, amely a GMT szerinti időt tartalmazza, a végén pedig egy „Z” áll. A „CCYY” karakterek a tranzakció évét jelölik, az „MM” karakterek a hónap számát annak tízes és egyes helyi értékével, a „DD” karakterek a hónap napját annak tízes és egyes helyi értékével, a „HH” karakterek az órát, az „MM” karakterek a percet, az „SS” karakterek pedig a másodpercet. A teljes dátum nem lehet későbbi az aktuális dátumnál.

4. **2. típusú logikai rekord: leíró szöveg**

E rekord nagy részének struktúráját nem az eredeti ANSI/NIST-szabvány határozza meg. E rekord az állományt küldő és fogadó szervezetek számára különös jelentőséggel bíró információkat tartalmaz. Az egymással kapcsolatban lévő daktiloszkópiai rendszerek kompatibilitásának biztosítása érdekében a rekord kizárólag az alább felsorolt mezőket tartalmazhatja. Itt kerül meghatározásra, hogy melyik mező kötelező, és melyik nem kötelező, valamint az egyes mezők struktúrája is.

4.1. A 2. típusú logikai rekord mezői

4.1.1. 2.001 mező: A logikai rekord hossza (Logical Record Length – LEN)

Ez a kötelező mező e 2. típusú rekord hosszát tartalmazza, valamint meghatározza a bájtok teljes számát, beleértve a rekordban tárolt minden mező minden karakterét és az adatelválasztókat is.

4.1.2. 2.002 mező: Képezonosító karakter (Image Designation Character – IDC)

Az e kötelező mezőben szereplő IDC az 1. típusú rekord állománytartalom (CNT) mezőjében (1003 mező) meghatározott IDC ASCII formátumban tárolt változata.

4.1.3. 2.003 mező: Rendszerinformáció (System Information – SYS)

Ez a kötelező mező négy bájt tartalmaz, amelyek azt jelölik, hogy ez a konkrét 2. típusú rekord az INT-I melyik verziójával kompatibilis.

Az első két bájt határozza meg a fő verziószámot, a második kettő pedig a másodlagos változatszámot. Ezen implementáció például az INT-I 4. verziójának 22. változatán alapul, így annak jelölése „0422” lenne.

4.1.4. 2.007 mező: Ügyszám (Case Number – CNO)

Ezt a számot a helyi daktiloszkópiai hivatal adja az egy bűncselekmény elkövetésének helyén gyűjtött látens képek összességének. Formátuma a következő: CC/szám

ahol CC az Interpol-országkód, amely két alfanumerikus karakter hosszúságú, a szám pedig összhangban van a vonatkozó helyi iránymutatásokkal, és legfeljebb 32 alfanumerikus karakter hosszúságú lehet.

E mező lehetővé teszi a rendszer számára az egy adott bűncselekménnyel kapcsolatos látens képek azonosítását.

**4.1.5. 2.008 mező: Sorozatszám (Sequence Number – SQN)**

Ez azonosítja az egy ügyszárhoz tartozó látens képek valamennyi sorozatát. Legfeljebb négy numerikus karakter hosszúságú lehet. Egy sorozat egy vagy több, a nyilvántartás és/vagy keresés céljából csoportként kezelt látens képet tartalmaz. E meghatározás értelmében a magukban álló látens képeket is el kell látni sorozatszámmal.

E mező és a MID (2.009 mező) együttes alkalmazása révén azonosítható a sorozaton belül egy adott látens kép.

**4.1.6. 2.009 mező: A látens kép azonosítója (Latent Identifier – MID)**

Ez azonosítja a sorozaton belül az adott látens képet. Értéke egy vagy két betű: az első látens kép jele az „A”, a másodiké a „B”, és így tovább, egészen „ZZ”-ig. E mezőt ugyanúgy kell alkalmazni, mint a látens képeknek az SQN (2.008 mező) leírásánál tárgyalt sorozatszámát.

**4.1.7. 2.010 mező: Bűnügyi nyilvántartási szám (Criminal Reference Number – CRN)**

Ez a nemzeti szervezet által azon személyeknek adott egyedi nyilvántartási szám, akiket első alkalommal vádolnak egy bűncselekmény elkövetésével. Egy országon belül egyetlen személy sem rendelkezhet egynél több CRN-nel, illetve több személynek nem lehet ugyanaz a CRN-e. Ugyanazon személy azonban több országban is rendelkezhet bűnügyi nyilvántartási számmal, amelyek között az országkód alapján lehet különbséget tenni.

A CRN mező formátuma a következő: CC/szám

ahol CC az ISO 3166 szerinti országkód, amely két alfanumerikus karakter hosszúságú, a szám pedig összhangban van a kibocsátó szervezet vonatkozó nemzeti iránymutatásaival, és legfeljebb 32 alfanumerikus karakter hosszúságú lehet.

A 2008/615/IB határozat szerinti tranzakciónál e mező a 4. típusú vagy 15. típusú rekordokban a képekhez kapcsolódó származási szervezet nemzeti bűnügyi nyilvántartási számát tartalmazza.

**4.1.8. 2.012 mező: Egyéb azonosítószám (Miscellaneous Identification Number – MN1)**

E mező a CPS vagy PMS tranzakció során továbbított CRN-t (2.010 mező) tartalmazza a bevezető országkód nélkül.

**4.1.9. 2.013 mező: Egyéb azonosítószám (Miscellaneous Identification Number – MN2)**

E mező az MPS vagy MMS tranzakció során továbbított CNO-t (2.007 mező) tartalmazza a bevezető országkód nélkül.

**4.1.10. 2.014 mező: Egyéb azonosítószám (Miscellaneous Identification Number – MN3)**

E mező az MPS vagy MMS tranzakció során továbbított SQN-t (2.008 mező) tartalmazza.

**4.1.11. 2.015 mező: Egyéb azonosítószám (Miscellaneous Identification Number – MN4)**

E mező az MPS vagy MMS tranzakció során továbbított MID-et (2.009 mező) tartalmazza.

**4.1.12. 2.063 mező: További információk (Additional Information – INF)**

Egy PMS kérelmet követő SRE tranzakció esetében e mező azon újra vonatkozó információkat tartalmaz, amely a lehetséges találatot (HIT) okozta. A mező formátuma:

NN ahol NN az ujjpozíció 5. táblázatban meghatározott kódja, amelynek hosszúsága két számjegy.

Ettől eltérő esetekben a mező nem kötelező. Legfeljebb 32 alfanumerikus karaktert tartalmaz, és további információkat szolgáltat a kérelemre vonatkozóan.

**4.1.13. 2.064 mező: A válaszadók listája (Respondents List – RLS)**

E mező legalább két almezőt tartalmaz. Az első almező a végrehajtott keresés típusát írja le a három betűből álló mnemonikus kóddal, amely a TOT mezőben (1004 mező) meghatározza a tranzakció típusát. A második almező egyetlen karaktert tartalmaz. „I” jelöli, ha a keresés eredményezett találatot (HIT), és „N” jelöli, ha a keresés nem talált egyezést (NOHIT). A harmadik almező a potenciális találat sorozatszámát és a potenciális találatok teljes számát tartalmazza, törtvonallal elválasztva. Ha több potenciális találat van, az eredmény több üzenet lesz.

Lehetséges találat (HIT) esetén a negyedik almező tartalmazza a legfeljebb hat számjegy hosszúságú pontszámot. Amennyiben a találat (HIT) megerősítést nyer, ezen almező értéke „999999” lesz.

Például: „CPS{RS}I{RS}001/001{RS}999999{GS}”

Amennyiben a távoli AFIS nem ad pontszámot, a megfelelő helyen nulla pontszámot kell alkalmazni.

#### 4.1.14. 2.074 mező: Állapotleíró üzenet/hibaüzenet mező (Status/Error Message Field – ERM)

E mező a tranzakciók által eredményezett hibaüzeneteket tartalmazza, amelyeket egy hibatranzakció részeként visszaküldenek a kérelmezőnek.

3. táblázat: Hibaüzenetek

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.

Hibaüzenetek a 100 és 199 közötti tartományban:

E hibaüzenetek az ANSI/NIST-rekordok ellenőrzésére vonatkoznak, felépítésük a következő:

<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>...

ahol

- error\_code: egy konkrét okra vonatkozó egyedi kód (lásd a 3. táblázatot),
- field\_id: a hibás mező ANSI/NIST szerinti mezőszáma (pl. 1.001, 2.001, ...) <record\_type>.field\_id>.sub\_field\_id> formátumban,
- dynamic text: a hiba részletesebb dinamikus leírása,
- LF: soremelés, amely egynél több hiba esetén a hibákat elválasztja egymástól,
- 1. típusú rekordnál az IDC értéke „-1”.

Például:

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

E mező minden hiba tranzakció esetében kötelező.

4.1.15. 2.320 mező: A potenciális találatok várható száma (Expected Number of Candidates – ENC)

E mező az ellenőrizendő potenciális találatoknak a kérelmező szervezet által várt legnagyobb számát tartalmazza. Az ENC értéke nem lehet nagyobb a 11. táblázatban meghatározott értékeknél.

5. **4. típusú logikai rekord: nagy felbontású szürkeárnyalatos kép**

Megjegyzendő, hogy a 4. típusú rekordok inkább bináris, mint ASCII szerinti jellemzőkkel bírnak. Így a rekordon belül minden mezőhöz tartozik egy megadott pozíció, következésképpen valamennyi mező kötelező.

A szabvány lehetővé teszi mind a kép méretének, mind felbontásának a rekordon belüli meghatározását. A szabvány értelmében a 4. típusú logikai rekordoknak daktiloszkópiai képadatokat kell tartalmazniuk, amelyek 500–520 pixel/hüvelyk névleges pixelsűrűséggel kerülnek továbbításra. Az új képek esetében a preferált arány 500 pixel/hüvelyk vagy 19,68 pixel/mm pixelsűrűség. Az INT-I 500 pixel/hüvelyk pixelsűrűséget ír elő, kivéve azt az esetet, ha hasonló rendszerek nem preferált, az 500–520 pixel/hüvelyk tartományon belüli felbontást használnak az egymás közötti kommunikációban.

5.1. A 4. típusú logikai rekord mezői

5.1.1. 4.001 mező: A logikai rekord hossza (Logical Record Length – LEN)

Ez a négybájtos mező e 4. típusú rekord hosszát tartalmazza, valamint meghatározza a bájtok teljes számát, beleértve a rekordban tárolt minden mező minden bájtyát.

5.1.2. 4.002 mező: Képezonosító karakter (Image Designation Character – IDC)

Ez a fejállományban megadott IDC-szám egybájtos, bináris formátumú változata.

5.1.3. 4.003 mező: A nyomat típusa (Impression Type – IMP)

A nyomat típusa egy egybájtos mező, amely a rekord hatodik bájtyát foglalja el.

4. táblázat: Az ujjnyomat típusa

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. 4.004 mező: Ujjpozíció (Finger Position – FGP)

Ez a 6 bájtos rögzített hosszú mező a 4. típusú rekord 7–12. báját foglalja el. A lehetséges ujjpozíciókat tartalmazza, a bal szélén lévő bájttól (a rekord 7. bájta) kezdve. Az ismert vagy legvalószínűbb ujjpozíció kódját az 5. táblázatból kell venni. Legfeljebb öt további ujjra lehet hivatkozni a többi ujjpozíciónak a fennmaradó öt bájta ugyanilyen formátumban történő bevitelével. Ha ötnél kevesebb ujjpozícióra történik hivatkozás, a kihasználatlan bájtokat bináris 255-tel kell feltölteni. A valamennyi ujjpozícióra való hivatkozáshoz a 0-át, az ismeretlen ujjpozíció kódját kell alkalmazni.

5. táblázat: Az ujjpozíciók kódja és maximális mérete

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

A bűncselekmények elkövetésének helyén gyűjtött látens képek esetében csak a 0–10 kódok használhatók.

#### 5.1.5. 4.005 mező: A képek szkennelési felbontása (Image Scanning Resolution – ISR)

Ez az egybájtos mező a 4. típusú rekord 13. báját foglalja el. Ha a tartalma „0”, akkor a kép mintavételezése a 19,68 pixel/mm (500 pixel/hüvelyk) preferált szkennelési arány alkalmazásával történt. Ha a tartalma „1”, akkor a kép mintavételezése az 1. típusú rekordban meghatározott alternatív szkennelési arány alkalmazásával történt.

#### 5.1.6. 4.006 mező: A vízszintes vonalak hossza (Horizontal Line Length – HLL)

E mező a 4. típusú rekord 14. és 15. bájtaán helyezkedik el. Az egyes letapogatási sorokban található pixelek számát határozza meg. Az első bájta bír a legnagyobb jelentőséggel.

## 5.1.7. 4.007 mező: A függőleges vonalak hossza (Vertical Line Length – VLL)

E mező a 16. és 17. bájton azt a számot adja meg, hogy a kép hány letapogatási sort tartalmaz. Az első bájtnál a legnagyobb jelentőséggel.

## 5.1.8. 4.008 mező: Szürkeárnyalatos tömörítési algoritmus (Gray-scale Compression Algorithm – GCA)

Ez az egybájtos mező határozza meg a képadatok kódolására használt szürkeárnyalatos tömörítési algoritmust. Ezen implementációban az „1” bináris kód jelöli a WSQ tömörítés (7. függelék) alkalmazását.

## 5.1.9. 4.009 mező: A kép (The Image)

E mező tartalmazza a képet leíró bájtfolyamot. Struktúrája természetesen az alkalmazott tömörítési algoritmustól függ.

## 6. 9. típusú logikai rekord: Minucia rekord

A 9. típusú rekordok olyan ASCII szöveget tartalmaznak, amely a látens képek alapján kódolt minuciákat és a vonatkozó információkat írja le. A látens képek keresésére vonatkozó tranzakciók esetében nincs korlátozva, hogy egy állományban hány 9. típusú rekord lehet, amelyek mindegyike más nézetre vagy látens képre vonatkozik.

## 6.1. A minuciák kiolvasása

## 6.1.1. A minucia típusának azonosítása

E szabvány három azonosítószámot határoz meg a minucia típusának meghatározására. Ezeket a 6. táblázat tartalmazza. A fodsorzál végződése az 1. típus. Az elágazás a 2. típus. Ha a minuciát nem lehet egyértelműen besorolni a fenti két típus valamelyikébe, akkor „egyéb” („other”), 0. típusú lesz.

6. táblázat: Minuciatípusok

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

## 6.1.2. A minucia elhelyezkedése és típusa

Annak érdekében, hogy a sablonok megfeleljenek az ANSI INCITS 378-2004 szabvány 5. szakaszának, a következő, a jelenlegi INCITS 378-2004 szabványt kibővítő módszert kell alkalmazni az egyes minuciák elhelyezkedésének (pozíció és irányszög) meghatározására.

A fodsorzál-végződés típusú minucia pozíciója a völgy középvonalának közvetlenül a fodsorzál végződése előtti elágazási pontja. Ha a völgy három ágát egy egyetlen pixel szélességű vonallá vékonyítjuk, a metszéspont adja a minucia pozícióját. Hasonlóképpen, az elágazás típusú minucia pozíciója a fodsorzál középvonalának elágazási pontja. Ha a fodsorzál három ágát egy egyetlen pixel szélességű vonallá vékonyítjuk, a három ág metszéspontja adja a minucia pozícióját.

Miután valamennyi fodsorzál-végződést elágazássá alakították, a daktiloszkópiai kép valamennyi minuciája elágazásként jelenik meg. Az egyes minuciák három ága metszéspontjának X és Y pixelkoordinátái közvetlenül formázhatók. A minucia irányultsága a vonal elágazásai alapján határozható meg. Meg kell vizsgálni minden elágazás három ágát, és meg kell határozni minden ág végpontját. A 6.1.2. ábra mutatja az ágak végének meghatározására használatos három módszert 500 ppi szkennelési felbontás mellett.

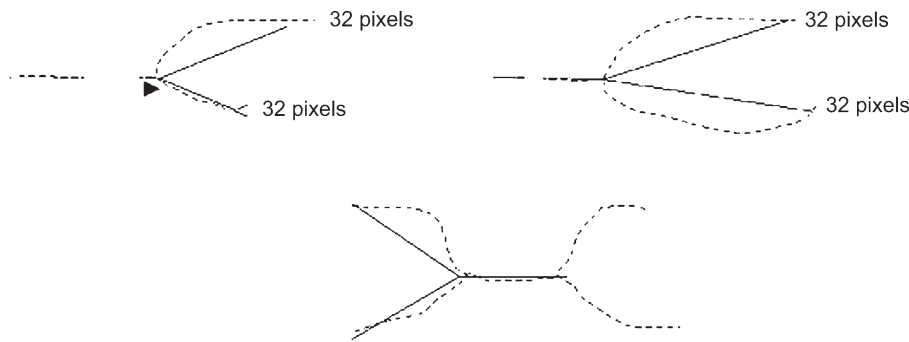
A végződés az elsőként bekezdés szerinti nyer megállapítást. A pixelszám 500 ppi szkennelési felbontáson alapul. A különböző szkennelési felbontások különböző pixelszámot vonnak maguk után.

— 0,064” távolság (a 32. pixel),

— A vonal egy ágának 0,02” és 0,064” távolság közötti végződése (a 10-től a 32. pixelig); az ettől rövidebb ágakat figyelmen kívül kell hagyni,

— Egy második elágazás történik 0,064” távolságon belül (a 32. pixel előtt).

6.1.2. ábra



A minuciák szögének megállapításához az elágazási pontban három virtuális félegyeneset hozunk létre, és meghosszabbítjuk azokat az egyes ágak végéig. A félegyenesek által közrefogott három szög legkisebbikének felezője mutatja meg a minucia irányultságát.

### 6.1.3. Koordináta-rendszer

Az ujjnyomatok minuciáinak ábrázolására karteziánus koordináta-rendszert használunk. A minuciák pozícióját azok  $x$  és  $y$  koordinátái adják meg. A koordináta-rendszer origója az eredeti kép bal felső sarka, az  $x$  tengely jobbra, az  $y$  pedig lefelé nő. A minuciák  $x$  és  $y$  koordinátáit az eredeti kép pixel egységeiben kell kifejezni. Megjegyzendő, hogy az origó helye és a mértékegységek nem felelnek meg az ANSI/NIST-ITL 1-2000 szabványban a 9. típusú rekordra vonatkozóan adott meghatározásokban használt megállapodásnak.

### 6.1.4. A minuciák irányultsága

A szögek szabványos matematikai formában vannak feltüntetve, ahol a nulla fok a jobb oldalon található, a szögek pedig az óramutató járásával ellentétes irányban növekednek. A jelölt szögek irányultsága a fodorszálak végződése esetén visszafelé mutat a fodorszál mentén, elágazás esetén pedig a völgy közepe felé. Ez a módszer 180 fokkal eltér az ANSI/NIST-ITL 1-2000 szabványban a 9. típusú rekordra vonatkozóan adott meghatározásokban használt, szögekre irányuló megállapodástól.

## 6.2. Az INCITS-378 formátumú 9. típusú logikai rekord mezői

A 9. típusú rekordok valamennyi mezőjébe ASCII szöveget kell bevinni. E címkézett mező típusú rekordban nem szerepelhet bináris mező.

### 6.2.1. 9.001 mező: A logikai rekord hossza (Logical record length – LEN)

Ez a kötelező ASCII mező a logikai rekord hosszát tartalmazza, valamint meghatározza a bájtok teljes számát, beleértve a rekordban tárolt minden mező minden karakterét.

### 6.2.2. 9.002 mező: Képzazonosító karakter (Image designation character – IDC)

Ez a kötelező kétbájtos mező a minucia-adatok meghatározását és pozícióját tartalmazza. Az e mezőben foglalt IDC megegyezik az 1. típusú rekord „állománytartalom” mezőjében található IDC-vel.

### 6.2.3. 9.003 mező: A nyomtatási típusa (Impression type – IMP)

Ez a kötelező egybájtos mező írja le a daktiloszkópiai képre vonatkozó információ kinyerésének a módját. A 4. táblázatból kiválasztott megfelelő kód ASCII szerinti értékét kell bevinni ebbe a mezőbe a nyomtatási típusának jelölésére.

### 6.2.4. 9.004 mező: A minuciák formátuma (Minutiae format – FMT)

E mező tartalma „U”, ami azt jelenti, hogy a minuciák formátuma megfelel az M1-378 követelményeinek. A 9. típusú rekord valamennyi adatmezőjének ASCII szövegmezőnek kell maradnia még akkor is, ha az adatok az M1-378 szabvány szerint lettek kódolva.

### 6.2.5. 9.126 mező: CBEFF-adatok (CBEFF information)

E mező három adatelemet tartalmaz. Az első adatelem a „27” (0x1B) értéket veszi fel. Ez a Biometriai Ipar Nemzetközi Szövetsége (International Biometric Industry Association – IBIA) által a CBEFF formátum tulajdonosának, az INCITS M1 technikai bizottságának adott azonosító. Az <US> karakter választja el ezt az elemet a CBEFF formátum típusától, amely az „513” (0x0201) értéket veszi fel annak jelölésére, hogy e rekord

csupán a pozícióra és az irányszögre vonatkozó adatokat tartalmaz a kiterjesztett adatblokkal kapcsolatos információk nélkül. Az <US> karakter választja el ezt az elemet a CBEFF termékazonosítótól (PID), amely a kódolóberendezés „tulajdonosát” határozza meg. Ezen értéket a gyártó állapítja meg. Az IBIA honlapjáról ([www.ibia.org](http://www.ibia.org)) lehet azt beszerezni, amennyiben fel van tüntetve.

- 6.2.6. 9.127 mező: A képrögzítő berendezés azonosítója (Capture equipment identification)

E mezőben az <US> karakterrel elválasztott két adatelem található. Az első tartalma „APPF”, ha a képrögzítésre eredetileg használt berendezés rendelkezik azt igazoló tanúsítvánnyal, hogy megfelel a CJIS-RS-0010 – a Szövetségi Nyomozóiroda (FBI) elektronikus ujjnyomat-továbbítási előírásai – F. függelékének (IAFIS képminőségi előírás, 1999. január 29.). Ha a berendezés annak nem felel meg, az adatelem értéke „NONE”. A második adatelem a képrögzítő berendezés azonosítóját tartalmazza, amely a képrögzítő berendezésnek a gyártó által adott termék száma. A „0” érték jelzi, hogy nem áll rendelkezésre a képrögzítő berendezés azonosítója.

- 6.2.7. 9.128 mező: A vízszintes vonalak hossza (Horizontal line length – HLL)

Ez a kötelező ASCII mező tartalmazza a továbbított kép egy vízszintes vonalán található pixelek számát. A legnagyobb vízszintes hossz 65 534 pixel lehet.

- 6.2.8. 9.129 mező: A függőleges vonalak hossza (Vertical line length – VLL)

Ez a kötelező ASCII mező tartalmazza a továbbított képben található vízszintes vonalak számát. A legnagyobb függőleges hossz 65 534 pixel lehet.

- 6.2.9. 9.130 mező: Egységtávolságok (Scale units – SLC)

Ez a kötelező ASCII mező határozza meg a kép mintavételezési frekvenciájának (pixelsűrűség) leírására használt egységtávolságokat. Ebben a mezőben az „1”-es a pixel/hüvelyket, a „2”-es pedig a pixel/centimétert jelöli. A mezőben a „0” azt jelzi, hogy nem adtak meg egységtávolságot. Ebben az esetben a HPS/VPS hányados adja meg a pixelarányt.

- 6.2.10. 9.131 mező: Egységnyi vízszintes pixelszám (Horizontal pixel scale – HPS)

Ez a kötelező ASCII mező határozza meg a vízszintes pixelsűrűséget egész számban, feltéve hogy az egységtávolságnál „1”-es vagy „2”-es szerepel. Ettől eltérő esetben a pixelarány vízszintes összetevőjét jelöli.

- 6.2.11. 9.132 mező: Egységnyi függőleges pixelszám (Vertical pixel scale – VPS)

Ez a kötelező ASCII mező határozza meg a függőleges pixelsűrűséget egész számban, feltéve hogy az egységtávolságnál „1”-es vagy „2”-es szerepel. Ettől eltérő esetben a pixelarány függőleges összetevőjét jelöli.

- 6.2.12. 9.133 mező: Az ujjról készült nézetek (Finger view)

Ez a kötelező mező tartalmazza az e rekord adataihoz társított ujjról készült nézetek számát. A nézetek száma „0”-val kezdődik, és egyesével nő „15”-ig.

- 6.2.13. 9.134 mező: Ujjpozíció (Finger position – FGP)

Ez a mező tartalmazza azt az ujjpozíciót jelölő kódot, amely a 9. típusú rekordban szereplő információt eredményezte. Az 5. táblázatból vett 1 és 10 közötti kódot vagy a 10. táblázatból vett megfelelő tenyérkódot kell használni az ujj- vagy a tenyérpozíciók jelölésére.

- 6.2.14. 9.135 mező: Az ujjak minősége (Finger quality)

Ez a mező tartalmazza az ujjakra vonatkozó összes minucia-adat minőségét, 0 és 100 közötti számjeggy megadásával. Ez a szám fejezi ki összességében az ujjakra vonatkozó rekord minőségét, valamint megmutatja az eredeti képnek, a minuciák kiolvasásának a minőségét és minden egyéb olyan műveletet, amely hatással lehet a minuciarekordra.

- 6.2.15. 9.136 mező: A minuciák száma (number of minutiae)

Ez a kötelező mező tartalmazza az ebben a logikai rekordban rögzített minuciák összesített számát.



## 6.2.16. 9.137 mező: Az ujjakra vonatkozó minucia-adatok (Finger minutiae data)

Ebben a kötelező mezőben az <US> karakterrel elválasztott, hat adatelem található. Több almezőből áll, amelyek mindegyike egy-egy minucia adatait tartalmazza. A minucia-almezők teljes számának meg kell egyeznie a 136. mezőben található végösszeeggel. Az első adatelem a minuciák indexszáma, amelynek kezdőértéke „1”, és az ujjnyomathoz kapcsolódó minden további minucia esetében „1”-gyel növekszik. A második és harmadik adatelem a minuciák „x” koordinátája és „y” koordinátái pixel egységben kifejezve. A negyedik adatelem a minuciák két fokok egységeiben rögzített szöge. Ez az érték 0 és 179 közötti nemnegatív szám. Az ötödik adatelem a minucia típusa. A „0”-ás értéket az „EGYÉB” típusú minucia feltüntetésére használják, az „1”-es értéket a fodorszálak végződéseire, a „2”-es értéket pedig a fodorszálak elágazásaira. A hatodik adatelem mutatja az egyes minuciák minőségét. Ez az érték minimum 1-től maximum 100-ig terjedhet. A „0”-ás érték azt jelzi, hogy nem áll rendelkezésre minőségre jellemző érték. Az egyes almezőket az <RS> elválasztó karakter segítségével kell elválasztani egymástól.

## 6.2.17. 9.138 mező: A fodorszálak számára vonatkozó információ (Ridge count information)

Ez a mező egy sor almezőből áll, amelyek mindegyike három adatelemet tartalmaz. Az első almező első adateleme mutatja a fodorszálak számának kiolvasási módszerét. A „0” azt jelzi, hogy nem kívánják feltüntetni a fodorszálak számának kiolvasására alkalmazott módszert, sem pedig azok sorrendjét a rekordban. Az „1” jelzi minden központi minucia esetén, hogy a legközelebbi minucia pontokig a fodorszálak számát meghatározták a négy negyedben, és minden központi minuciához tartozó fodorszál számot együtt sorolnak fel. A „2” jelzi minden központi minucia esetén, hogy a legközelebbi minucia pontokig a fodorszálak számát meghatározták a nyolc nyolcadban, és minden központi minuciához tartozó fodorszál számot együtt sorolnak fel. Az első almező mindkét fennmaradó adateleme „0”-t tartalmaz. Az adatelemeket az <US> elválasztó karakter választja el egymástól. Az ezután következő almezők első adatelemként a központi minuciák indexszámát, második adatelemként a szomszédos minuciák indexszámát, harmadik adatelemként pedig a keresztezett fodorszálak számát tartalmazzák. Az almezőket az <RS> elválasztó karakter választja el egymástól.

## 6.2.18. 9.139 mező: Az alappontra vonatkozó információ (Core information)

Ez a mező annyi almezőt foglal magában, ahány alappont az eredeti képen található. Mindegyik almező három adatelemből áll. Az első két adatelem az „x” és „y” koordináták által meghatározott helyzetet tartalmazza pixel egységben kifejezve. A harmadik adatelem az alappont két fokok egységeiben rögzített szögét tartalmazza. Ez az érték 0 és 179 közötti nemnegatív szám. Több alappontot az <RS> elválasztó karakter választ el egymástól.

## 6.2.19. 9.140 mező: A deltára vonatkozó információ (Delta information)

Ez a mező annyi almezőt foglal magában, ahány delta az eredeti képen található. Mindegyik almező három adatelemből áll. Az első két adatelem az „x” és „y” koordináták által meghatározott helyzetet tartalmazza pixel egységben kifejezve. A harmadik adatelem a delta két fokok egységeiben rögzített szögét tartalmazza. Ez az érték 0 és 179 közötti nemnegatív szám. Több alappontot az <RS> elválasztó karakter választ el egymástól.

## 7. A 13. típusú, változó felbontású látens kép-rekord

A 13. típusú címkéztetmező-logikairekord a látens képekből kinyert képadatokat tartalmazza. Ezeket a képeket a tervek szerint szervezetekhez továbbítják, amelyek gépi módon vagy emberi közreműködéssel elvégzik a keresett jellemzők képekből történő kiolvasását.

Az alkalmazott szkennelési felbontásra, a képméretre vonatkozó információkat és a képfeldolgozáshoz szükséges egyéb paramétereket címkéztet mezőként rögzítik a rekordban.

7. táblázat: A 13. típusú, változó felbontású látens kép-rekord szerkezete

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	—

Jelmagyarázat a karaktertípusokhoz: N = numerikus; A = alfabetikus; AN = alfanumerikus; B = bináris

#### 7.1. A 13. típusú logikai rekord mezői

A következő bekezdések ismertetik a 13. típusú logikai rekord egyes mezőiben tárolt adatokat.

A 13. típusú logikai rekordban a bejegyzések számozott mezőkben jelennek meg. Szükséges, hogy a rekord első két mezője sorrendben, a képadatokot tartalmazó mező pedig az utolsó tényleges mezőként szerepeljen a rekordban. A 13. típusú rekord minden mezőjére vonatkozóan a 7. táblázat felsorolja a „feltételkódot” – azaz kötelező „M – Mandatory” vagy nem kötelező „O – Optional” –, a mező számát, a mező nevét, a karaktertípust, a mező méretét és az előfordulási határokat. A háromjegyű mezőszám alapján a mező maximális bájtszám szerinti méretét az utolsó oszlopban adják meg. Ha a mezőszámhoz több számjegyet használnak fel, akkor a maximális bájtszám is nőni fog. Az „előfordulás szerinti mezőméret” két bejegyzése tartalmazza a mezőben használt összes elválasztó karaktert. A „maximális bájtszám” tartalmazza a mezőszámot, az adatot és az összes elválasztó karaktert, beleértve a „GS” karaktert is.

##### 7.1.1. 13.001 mező: A logikai rekord hossza (Logical record length – LEN)

Ez a kötelező ASCII mező tartalmazza a 13. típusú logikai rekordban található bajtok számát. A 13.001 mező határozza meg a rekord hosszát, beleértve a rekordban tárolt minden mező minden karakterét és az adatelválasztókat is.

##### 7.1.2. 13.002 mező: Képezonosító karakter (Image designation character – IDC)

Ezt a kötelező ASCII mezőt a rekordban tárolt látenskép-adatok azonosítására használják. Ez az IDC megegyezik az 1. típusú rekord „állománytartalom” (CNT) mezőjében található IDC-vel.

##### 7.1.3. 13.003 mező: A nyomtat típusa (Impression type – IMP)

Ez a kötelező egy- vagy kétbájtos ASCII mező jelzi a látens képre vonatkozó információ kinyerésének a módját. A 4. táblázatból (ujj) vagy 9. táblázatból (tenyér) választott megfelelő, látens képre vonatkozó kódot kell bevinni ebbe a mezőbe.

7.1.4. 13.004 mező: származási szervezet/ORI (Source agency/ORI – SRC)

Ez a kötelező ASCII mező tartalmazza azon hatóságnak vagy szervezetnek a nevét, amely eredetileg rögzítette a rekordban tárolt arcképet. Általában a képet rögzítő szervezet származási szervezet azonosítója (ORI) szerepel ebben a mezőben. Két adatelemből áll, és formátuma a következő: CC/szervezet.

Az első adatelem tartalmazza az Interpol országcódját (CC), amely két alfanumerikus karakter hosszú. A második elem – a szervezet – szabad szövegű meghatározás legfeljebb 32 alfanumerikus karakterig.

7.1.5. 13.005 mező: A látens kép rögzítésének időpontja (Latent capture date – LCD)

Ez a kötelező ASCII mező tartalmazza azt az időpontot, amikor a rekordban tárolt látens képet rögzítették. Az időpont a nyolc számjegyű CCYYMMDD formátumban jelenik meg. A CCYY karakterek mutatják a kép rögzítésének évét, az MM karakterek a hónap sorszámát jelölik annak tízes és egyes helyi értékével, a DD karakterek pedig az adott hónap napját annak tízes és egyes helyi értékével. Például 20000229 az 2000. február 29. A teljes dátumnak valós időpontnak kell lennie.

7.1.6. 13.006 mező: A vízszintes sorok hossza (Horizontal line length – HLL)

Ez a kötelező ASCII mező tartalmazza a továbbított kép egy vízszintes során található pixelek számát.

7.1.7. 13.007 mező: A függőleges sorok hossza (Vertical line length – VLL)

Ez a kötelező ASCII mező tartalmazza a továbbított képben található vízszintes sorok számát.

7.1.8. 13.008 mező: Egységtávolságok (Scale units – SLC)

Ez a kötelező ASCII mező határozza meg a kép mintavételezési frekvenciájának (pixelsűrűség) leírására használt egységtávolságokat. Ebben a mezőben az „1”-es a pixel/hüvelyket, a „2”-es pedig a pixel/centimétert jelöli. A mezőben a „0” azt jelzi, hogy nem adtak meg egységtávolságot. Ebben az esetben a HPS/VPS hányados adja meg a pixelarányt.

7.1.9. 13.009 mező: Egységnyi vízszintes pixelszám (Horizontal pixel scale – HPS)

Ez a kötelező ASCII mező határozza meg a vízszintes pixelsűrűséget egész számban, feltéve hogy az egységtávolságnál „1”-es vagy „2”-es szerepel. Ettől eltérő esetben a pixelarány vízszintes összetevőjét jelöli.

7.1.10. 13.010 mező: Egységnyi függőleges pixelszám (Vertical pixel scale – VPS)

Ez a kötelező ASCII mező határozza meg a függőleges pixelsűrűséget egész számban, feltéve hogy az egységtávolságnál „1”-es vagy „2”-es szerepel. Ettől eltérő esetben a pixelarány függőleges összetevőjét jelöli.

7.1.11. 13.011 mező: Tömörítési algoritmusok (Compression algorithm – CGA)

Ez a kötelező ASCII mező határozza meg a szürkeárnyaltos képek tömörítésére használt algoritmust. A tömörítési kódokat illetően lásd a 7. függelékét.

7.1.12. 13.012 mező: Bit/pixel (Bits per pixel – BPX)

Ez a kötelező ASCII mező tartalmazza az egy pixel ábrázolásához használt bitek számát. Ez a mező a „0”-tól „255”-ig terjedő átlagos szürkeárnyaltos értékek esetében „8”-as bejegyzést tartalmaz. E mezőben a „8”-asnál nagyobb bejegyzés nagyobb pontosságú szürkeárnyaltos pixelt jelöl.

7.1.13. 13.013 mező: Ujj-/tenyérpozíció (Finger/palm position – FGP)

Ez a kötelező címkézett mező a látens képpel esetleg egyező, egy vagy több ujj- vagy tenyérpozíciót tartalmaz. Az ismert vagy legvalószínűbb ujjpozíciónak megfelelő decimális kódszámot az 5. táblázatból, illetve a legvalószínűbb tenyérpozícióét a 10. táblázatból kell venni, és egy- vagy kétkarakters formában kell bevinni az ASCII almezőbe. További ujj- és/vagy tenyérpozíciókra lehet hivatkozni a változó pozíciókódoknak az „RS” elválasztó karakterrel elválasztott almezőbe történő bevitelével. Az „Ismeretlen ujj”-hoz rendelt „0”-ás kód referenciaként szolgál minden ujjpozícióhoz egytől tízig. Az „Ismeretlen tenyér”-hez rendelt „20”-as kód referenciaként szolgál minden felsorolt tenyérpozícióhoz.

7.1.14. 13.014-019 mező: Jövőbeli definíciónak fenntartva (Reserved for future definition – RSV)

Ezeket a mezőket e szabvány jövőbeli felülvizsgálatait követő beillesztésük céljára tartják fenn. E mezők egyike sem használatos ezen a felülvizsgálati szinten. Ilyen mezők előfordulása esetén figyelmen kívül kell őket hagyni.

**7.1.15. 13.020: Megjegyzés (Comment – COM)**

Ez a nem kötelező mező megjegyzéseknek vagy egyéb ASCII szöveges információnak a látenskép-adatokkal együtt történő beszurására szolgálhat.

**7.1.16. 13.021-199 mező: Jövőbeli definíciónak fenntartva (Reserved for future definition – RSV)**

Ezeket a mezőket e szabvány jövőbeli felülvizsgálatait követő beillesztésük céljára tartják fenn. E mezők egyike sem használatos ezen a felülvizsgálati szinten. Ilyen mezők előfordulása esetén figyelmen kívül kell őket hagyni.

**7.1.17. 13.200-998 mező: Felhasználói mezők (User-defined fields – UDF)**

Ezeket a mezőket a felhasználók határozzák meg, és jövőbeli követelményekhez használatosak. Méretüket és tartalmukat a felhasználó határozza meg, összhangban a fogadó szervezettel. Előfordulásuk esetén ASCII szöveges információt tartalmaznak.

**7.1.18. 13.999 mező: Képadatok (Image data – DAT)**

E mező a rögzített látens kép valamennyi adatát tartalmazza. Mindig a „999”-es mezőszámot kapja, és az utolsó tényleges mezőként kell szerepelnie a rekordban. Például a „13.999”-et binárisan ábrázolt képadat követi.

A tömörítetlen szürkeárnyaltos képadatokat pixelenként általában az egy bájtot kitevő nyolc bitre kvantálják (256 szürkességi szint). Amennyiben a BPX-re vonatkozó 13012 mezőben található bejegyzés „8”-nál nagyobb vagy kisebb, az egy pixel tárolásához szükséges bájtok száma eltérő lesz. Tömörítés esetén a pixeladatokat a CGA mezőben meghatározott tömörítési technikának megfelelően tömörítik.

**7.2. A 13. típusú, változó felbontású látenskép-rekord vége**

Az egységesség érdekében a 13.999 mező utolsó adatbájtját követően közvetlenül egy „FS” elválasztó karaktert használnak a következő logikai rekordtól való elválasztás céljából. Ezt az elválasztót bele kell számítani a 13. típusú rekord mezőhosszába.

**8. A 15. típusú, változó felbontású tenyérynymatkép-rekord**

A 15. típusú címkézettmező-logikairekord tenyérynymatkép-adatokat tartalmaz, és ezen adatoknak a digitalizált képre vonatkozó állandó és felhasználói szöveges információs mezőkkel együtt történő cseréjére szolgál. Az alkalmazott szkennelési felbontásra, a képméretre vonatkozó információkat és a képfeldolgozáshoz szükséges egyéb paramétereket vagy megjegyzéseket címkézett mezőként rögzítik a rekordban. A más szervezetekhez továbbított tenyérynymat-képeket a fogadó szervezetek dolgozzák fel annak érdekében, hogy összehasonlítási céllal kiolvassák a keresett jellemzőket.

A képadatok megszerzhetőek közvetlenül az érintettől képolvasó-eszköz (live-scan device) használatával, illetve tenyérynymat-kártyáról vagy az érintett tenyérynymatát tároló egyéb médiahordozóról.

A tenyérynymat-képek megszerzésére használt bármely módszerrel képsorozat rögzíthető mindegyik kézzől. Ez a sorozat tartalmazza a tenyér írás közben lefelé tartott részét egy szkennelt képen, valamint az egész tenyér teljes felületét a csuklótól az ujjak hegyéig egy vagy két szkennelt képen. Ha két kép szolgál az egész tenyér ábrázolására, akkor az alsó kép a csuklótól az ujjak közötti terület felső részéig (harmadik ujjperc) terjed, és magában foglalja a tenyér felületén a hüvelykujj izompárnáját és a kisujj izompárnáját. A felső kép az ujjak közötti terület alsó részétől az ujjak hegyéig terjed. Ez elegendő átfedést nyújt a két kép között, amelyek mindegyike az ujjak közötti terület feletti részre irányul. Az e közös területen található fodorszálak struktúrájának és részleteinek összehasonlításával a vizsgálatot végző személy biztonsággal meg tudja állapítani, hogy mindkét kép ugyanarról a tenyerről készült-e.

Mivel egy tenyérynymat rögzítésének eredményeit különböző célokra lehet használni, ezért a tenyerről vagy kézzől készült adatrögzítés egy vagy több egyedi képterületet is tartalmazhat. Egy személy esetében a teljes tenyérynymatrekord-sorozat általában tartalmazza a tenyér írás közben lefelé tartott részéről és mindegyik kéz egész tenyeréről készült képe(ke)t. Mivel a címkézett mező típusú logikai képrekordok csak egy bináris mezőt tartalmazhatnak, egy 15. típusú rekord szükséges a tenyér írás közben lefelé tartott részéhez, egy vagy két 15. típusú rekord pedig az egész tenyérhez. Négy-hat 15. típusú rekord szükséges ezért az érintett tenyérynymatainak egy átlagos tenyérynymat-rögzítéssel történő ábrázolásához.

**8.1. A 15. típusú logikai rekord mezői**

A következő bekezdések ismertetik a 15. típusú logikai rekord egyes mezőiben tárolt adatokat.

A 15. típusú logikai rekordban a bejegyzések számozott mezőkben jelennek meg. Szükséges, hogy a rekord első két mezője sorrendben, a képadatokat tartalmazó mező pedig az utolsó tényleges mezőként szerepeljen a rekordban. A 15. típusú rekord minden mezőjére vonatkozóan a 8. táblázat felsorolja a „feltételkódot” – azaz kötelező „M – Mandatory” vagy választható „O – Optional” –, a mező számát, a mező nevét, a karaktertípust, a mező méretét és az előfordulási határokat. A háromjegyű mezőszám alapján a mező maximális bájtszám szerinti méretét az utolsó oszlopban adják meg. Ha a mezőszámhoz több számjegyet használnak fel, akkor a maximális bájtszám is nőni fog. Az „előfordulás szerinti mezőméret” két bejegyzése tartalmazza a mezőben használt összes elválasztó karaktert. A „maximális bájtszám” tartalmazza a mezőszámot, az adatot és az összes elválasztó karaktert, beleértve a „GS” karaktert is.

8.1.1. 15.001 mező: A logikai rekord hossza (Logical record length – LEN)

Ez a kötelező ASCII mező tartalmazza a 15. típusú logikai rekordban található bájtok számát. A 15.001 mező határozza meg a rekord hosszát, beleértve a rekordban tárolt minden mező minden karakterét és az adatelválasztókat is.

8.1.2. 15.002 mező: Képezonosító karakter (Image designation character – IDC)

Ezt a kötelező ASCII mezőt a rekordban tárolt tenyérszámkép azonosítására használják. Ez az IDC megegyezik az 1. típusú rekord „állománytartalom” (CNT) mezőjében található IDC-vel.

8.1.3. 15.003 mező: A nyomtatási típusa (Impression type – IMP)

Ez a kötelező egybájtos ASCII mező jelzi a tenyérszámkép-re vonatkozó információ kinyerésének a módját. A 9. táblázatból választott megfelelő kódot kell bevinni ebbe a mezőbe.

8.1.4. 15.004 mező: származási szervezet/ORI (Source agency/ORI – SRC)

Ez a kötelező ASCII mező tartalmazza azon hatóságnak vagy szervezetnek a nevét, amely eredetileg rögzítette a rekordban tárolt arcképet. Általában a képet rögzítő szervezet származási szervezet azonosítója (ORI) szerepel ebben a mezőben. Két adatelemből áll, és formátuma a következő: CC/szervezet.

Az első adatelem tartalmazza az Interpol országkódját (CC), amely két alfanumerikus karakter hosszúságú. A második elem – a szervezet – szabad szövegű meghatározás legfeljebb 32 alfanumerikus karakterig.

8.1.5. 15.005 mező: A tenyérszámkép rögzítésének időpontja (Fingerprint capture date – PCD)

Ez a kötelező ASCII mező tartalmazza azt az időpontot, amikor a tenyérszámképet rögzítették. Az időpont a nyolc számjegyű CCYYMMDD formátumban jelenik meg. A CCYY karakterek mutatják a kép rögzítésének évét, az MM karakterek a hónap sorszámát jelölik annak tízes és egyes helyi értékével, a DD karakterek pedig az adott hónap napját annak tízes és egyes helyi értékével. Például a 20000229 bejegyzés az 2000. február 29. A teljes dátumnak valós időpontnak kell lennie.

8.1.6. 15.006 mező: A vízszintes sorok hossza (Horizontal line length – HLL)

Ez a kötelező ASCII mező tartalmazza a továbbított kép egy vízszintes során található pixelek számát.

8.1.7. 15.007 mező: A függőleges sorok hossza (Vertical line length – VLL)

Ez a kötelező ASCII mező tartalmazza a továbbított képben található vízszintes sorok számát.

8.1.8. 15.008 mező: Egységávolságok (Scale units – SLC)

Ez a kötelező ASCII mező határozza meg a kép mintavételezési frekvenciájának (pixelsűrűség) leírására használt egységávolságokat. Ebben a mezőben az „1”-es a pixel/hüvelyket, a „2”-es pedig a pixel/centimétert jelöli. A mezőben a „0” azt jelzi, hogy nem adtak meg egységávolságot. Ebben az esetben a HPS/VPS hányados adja meg a pixelarányt.

8.1.9. 15.009 mező: Egységnyi vízszintes pixelszám (Horizontal pixel scale – HPS)

Ez a kötelező ASCII mező határozza meg a vízszintes pixelsűrűséget egész számban, feltéve hogy az egységávolságnál „1”-es vagy „2”-es szerepel. Ettől eltérő esetben a pixelarány vízszintes összetevőjét jelöli.

8.1.10. 15.010 mező: Egységnyi függőleges pixelszám (Vertical pixel scale – VPS)

Ez a kötelező ASCII mező határozza meg a függőleges pixelsűrűséget egész számban, feltéve hogy az egységávolságnál „1”-es vagy „2”-es szerepel. Ettől eltérő esetben a pixelarány függőleges összetevőjét jelöli.

8. táblázat: A 15. típusú, változó felbontású tenyérsztyomat-rekord szerkezete

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	—

9. táblázat: A tenyérsztyomat típusa

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. 15.011 mező: Tömörítési algoritmusok (Compression algorithm – CGA)

Ez a kötelező ASCII mező határozza meg a szürkeárnyaltos képek tömörítésére használt algoritmust. Az e mezőbe történt „NONE” bejegyzés jelzi, hogy az e rekordban tárolt adatok nincsenek tömörítve. A tömörítendő képek esetében ez a mező tartalmazza a tízujjas ujjnyomat-képek tömörítésére preferált módszert. Az érvényes tömörítési kódok a 7. függelékben kerültek meghatározásra.

## 8.1.12. 15.012 mező: Bit/pixel (Bits per pixel – BPX)

Ez a kötelező ASCII mező tartalmazza az egy pixel ábrázolásához használt bitek számát. Ez a mező a „0”-tól „255”-ig terjedő átlagos szürkeárnyalatos értékek esetében „8”-as bejegyzést tartalmaz. Az e mezőben szereplő „8”-asnál nagyobb, illetve kisebb bejegyzés nagyobb, illetve kisebb pontosságú szürkeárnyalatos pixelt jelöl.

10. táblázat: Tenyérkódok, -felületek és -méretek

Palm Position	Palm code	Image area (mm <sup>2</sup> )	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. 15.013 mező: Tenyérnyomat-pozíció (Palmprint position – PLP)

Ez a kötelező címkézett mező tartalmazza azt a tenyérnyomat-pozíciót, amely egyezik a tenyérnyomat-képpel. Az ismert vagy legvalószínűbb tenyérnyomat-pozícióknak megfelelő decimális kódszámot a 10. táblázatból kell venni, és kétkarakters formában kell bevinni az ASCII almezőbe. A 10. táblázat továbbá felsorolja a lehetséges tenyérnyomat-pozíciókhoz tartozó legnagyobb képfelületeket és méreteket.

## 8.1.14. 15.014-019 mező: Jövőbeli definíciónak fenntartva (Reserved for future definition – RSV)

Ezeket a mezőket e szabvány jövőbeli felülvizsgálatait követő beillesztésük céljára tartják fenn. E mezők egyike sem használatos ezen a felülvizsgálati szinten. Ilyen mezők előfordulása esetén figyelmen kívül kell őket hagyni.

## 8.1.15. 15.020 mező: Megjegyzés (Comment – COM)

Ez a választható mező megjegyzéseknek vagy egyéb ASCII szöveges információknak a tenyérnyomatkép-adatokkal együtt történő beszúrására szolgálhat.

## 8.1.16. 15.021-199 mező: Jövőbeli definíciónak fenntartva (Reserved for future definition – RSV)

Ezeket a mezőket e szabvány jövőbeli felülvizsgálatait követő beillesztésük céljára tartják fenn. E mezők egyike sem használatos ezen a felülvizsgálati szinten. Ilyen mezők előfordulása esetén figyelmen kívül kell őket hagyni.

## 8.1.17. 15.200-998 mező: Felhasználói mezők (User-defined fields – UDF)

Ezeket a mezőket a felhasználók határozzák meg, és jövőbeli követelményekhez használatosak. Méretüket és tartalmukat a felhasználó határozza meg, összhangban a fogadó szervezettel. Előfordulásuk esetén ASCII szöveges információt tartalmaznak.

## 8.1.18. 15.999 mező: Képadatok (Image data – DAT)

E mező a rögzített tenyérnyomat-kép valamennyi adatát tartalmazza. Mindig a „999”-es mezőszámot kapja, és az utolsó tényleges mezőként kell szerepelnie a rekordban. Például a „15.999”-et binárisan ábrázolt képadat követi. A tömörítetlen szürkeárnyalatos képadatokat pixelenként általában az egy bájtot kitevő nyolc bitre kvantálják (256 szürkeségi szint). Amennyiben a BPX-re vonatkozó 15.012 mezőben található bejegyzés „8”-nál nagyobb vagy kisebb, az egy pixel tárolásához szükséges bájtok száma eltérő lesz. Tömörítés esetén a pixeladatokat a CGA mezőben meghatározott tömörítési technikának megfelelően tömörítik.

## 8.2. A 15. típusú, változó felbontású tenyérnyomatkép-rekord vége

Az egységesség érdekében a 15.999 mező utolsó adatbájtját követően közvetlenül egy „FS” elválasztó karaktert használnak a következő logikai rekordtól való elválasztás céljából. Ezt az elválasztót bele kell számítani a 15. típusú rekord mezőhosszába.

## 8.3. További 15. típusú, változó felbontású tenyérnyomatkép-rekordok

További 15. típusú rekordok vihetők be az állományba. Minden további tenyérnyomat-képhez az „FS” elválasztó karakterrel együtt egy teljes 15. típusú logikai rekordra van szükség.

11. táblázat: Az adattovábbításonként ellenőrzésre elfogadott kérelmek maximális száma

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

Keresési típusok:

TP/TP: tízujjasak között tízujjasra

LT/TP: tízujjasak között látens ujjnyomatra

LP/PP: tenyérnyomatok között látens tenyérnyomatra

TP/UL: azonosítatlan látens ujjnyomatok között tízujjasra

LT/UL: azonosítatlan látens ujjnyomatok között látens ujjnyomatra

PP/ULP: azonosítatlan látens tenyérnyomatok között tenyérnyomatra

LP/ULP: azonosítatlan látens tenyérnyomatok között látens tenyérnyomatra

9. **Függelékek a 2. fejezethez (daktiloszkópiai adatok cseréje)**

## 9.1. 1. függelék ASCII elválasztó kódok

ASCII	Position <sup>(1)</sup>	Description
LF	1/10	Separates error codes in field 2074
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

<sup>(1)</sup> Ez az ASCII szabványban meghatározott pozíció.

## 9.2. 2. függelék Az alfanumerikus ellenőrző karakter kiszámítása

A TCN és a TCR (1.09 és 1.10 mező) esetében:

Az ellenőrző karakternek megfelelő számot az alábbi képlet segítségével generálják:

$(YY * 10^8 + SSSSSSS) \text{ Modulo } 23$

A képletben YY az év utolsó két számjegyének, SSSSSSS pedig a sorozatszámnak a numerikus értéke.

Az ellenőrző karaktert ezután az alábbi kereső táblázatból generálják.



A CRO esetében (2.010 mező)

Az ellenőrző karakternek megfelelő számot az alábbi képlet segítségével generálják:

$(YY * 10^6 + NNNNNN) \text{ Modulo } 23$

A képletben YY az év utolsó két számjegyének, NNNNNN pedig a sorozatszámnak a numerikus értéke.

Az ellenőrző karaktert ezután az alábbi kereső táblázatból generálják.

Ellenőrzőkarakter-kereső táblázat

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. 3. függelék Karakterkódok

#### 7-bites ANSI-kód az információcsere céljára

ASCII Character Set

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

### 9.4. 4. függelék Tranzakcióáttekintés

#### 1. típusú rekord (kötelező)

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

A „Feltétel” oszlop alatt:

O = Optional – nem kötelező; M = Mandatory – kötelező; C = Conditional – feltételes, ha a tranzakció válasz a származási szervezetnek.

## 2. típusú rekord (kötelező)

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	—	—

A „Feltétel” oszlop alatt:

O = Optional – nem kötelező; M = Mandatory – kötelező; C = Conditional – feltételes, ha elérhetők az adatok

\* = ha az adattovábbítás a nemzeti jogszabályokkal összhangban történik (nem tartozik a 2008/615/IB határozat hatálya alá)

## 9.5. 5. függelék Az 1. típusú rekord definíciói

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

A „Feltétel” oszlop alatt: O = Optional – nem kötelező; M = Mandatory – kötelező; C = Conditional – feltételes

A „Karaktertípus” oszlop alatt: A = alfa, N = numerikus, B = bináris

1\* a szervezet nevében megengedett karakterek [„0..9”, „A..Z”, „a..z”, „\_”, „.”, „-”, „-”]

## 9.6. 6. függelék A 2. típusú rekord definíciói

## A.6.1. táblázat: CPS- és PMS-tranzakció

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}

A.6.2. táblázat: SRE-tranzakció

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

A.6.3. táblázat: ERR-tranzakció

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 2.003 INVALID SYSTEM INFORMATION {GS}

A.6.4. táblázat: MPS- és MMS-tranzakció

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

A „Feltétel” oszlop alatt: O = Optional – nem kötelező; M = Mandatory – kötelező; C = Conditional – feltételes

A „Karaktertípus” oszlop alatt: A = alfa, N = numerikus, B = bináris

1\* megengedett karakterek [„0..9”, „A..Z”, „a..z”, „\_” „.”, „-”, „-” „.”]

#### 9.7. 7. függelék: Szűrkeskála tömörítési kódok

Tömörítési kódok

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. 8. függelék: Levelezési előírások

A belső munkafolyamatok hatékonyabbá tétele érdekében levelezéskor a PRUEM tranzakciók esetén a „tárgy” mezőben szerepelnie kell azon tagállam országkódjának (CC), amely az üzenetet küldi, valamint a tranzakció típusának (TOT 1004 mező).

Formátum: CC/TOT

Például: „DE/CPS”

A levél üresen is elküldhető.

### 3. FEJEZET: A gépjármű-nyilvántartási adatok cseréje

#### 1. A gépjármű-nyilvántartási adatok automatizált keresésekor használt közös adatkészlet

##### 1.1. Fogalommeghatározások

A kötelező és nem kötelező adatoknak a 16. cikk (4) bekezdésében említett meghatározásai az alábbiak:

Kötelező (M):

Az adatot kötelező megadni, amennyiben az információ valamely tagállam nemzeti nyilvántartásában rendelkezésre áll. Az információcsere tehát kötelezettség, ha az adat rendelkezésre áll.

Nem kötelező (O):

Az adat megadható, amennyiben az információ valamely tagállam nemzeti nyilvántartásában rendelkezésre áll. Az információcsere tehát nem kötelezettség, még akkor sem, ha az adat rendelkezésre áll.

(Y) jelzés jelöli az adatkészlet minden olyan elemét, amelyet a 2008/615/IB határozat szempontjából fontos elemként külön meghatároztak.

##### 1.2. Gépjármű/tulajdonos/üzemben tartó keresése

###### 1.2.1. Keresés indítása

Két különböző módon lehet lekérdezni a következő bekezdésben meghatározott információkat:

- Az alvázszám (VIN), hivatkozási dátum és időpont (nem kötelező) alapján,
- A rendszám, az alvázszám (VIN) (nem kötelező), hivatkozási dátum és időpont (nem kötelező) alapján.

E keresési feltételek használatával a keresés eredményeként olyan információkat küldenek vissza, amelyek egy vagy időnként több gépjárműre vonatkoznak. Ha csak egyetlen gépjárműre vonatkozóan kell információt visszaküldeni, valamennyi adat egyetlen válaszban érkezik. Ha egynél több gépjármű szerepel a találatok között, a megkeresett tagállam maga döntheti el, hogy mely adatokat küldi vissza: valamennyi adatot vagy csak a keresés szűkítéséhez szükséges adatokat (például a magánélet védelme okán vagy a teljesítményhez kapcsolódó okokból).

A keresés szűkítéséhez szükséges adatok az 1.2.2.1. pont alatt szerepelnek. Az 1.2.2.2. pont ismerteti a teljes adatkészletet.

Ha a keresés alvázszám, hivatkozási dátum és időpont alapján történik, a részt vevő tagállamok egyikében vagy mindegyikében végrehajtható.

Ha a keresés rendszám, hivatkozási dátum és időpont alapján történik, azt egy konkrét tagállamra kell vonatkoztatni.

Alapesetben a keresés a tényleges dátum és időpont megadásával történik, de múltbeli hivatkozási dátum és időpont megadásával is lehetséges keresni. Ha a keresés múltbeli hivatkozási dátum és időpont megadásával történik, és az adott tagállam nyilvántartásában nem áll rendelkezésre korábbi információ, mivel ilyen információkat egyáltalán nem tartanak nyilván, a ténylegesen rendelkezésre álló információ visszaküldhető annak feltüntetésével, hogy az aktuális információ.

###### 1.2.2. Adatkészlet

###### 1.2.2.1. A keresés szűkítéséhez szükséges, visszaküldendő adatok

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

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

<sup>(1)</sup> M = kötelező, amennyiben a nemzeti nyilvántartásban rendelkezésre áll, O = nem kötelező.

<sup>(2)</sup> A tagállamok által az adatokhoz külön hozzárendelt jellemzőket Y jelzi.

<sup>(3)</sup> Harmonizált okmánykód, lásd az 1999. április 29-i 1999/37/EK tanácsi irányelvet.

#### 1.2.2.2. Teljes adatkészlet

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

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



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

<sup>(1)</sup> M = kötelező, amennyiben a nemzeti nyilvántartásban rendelkezésre áll, O = nem kötelező.

<sup>(2)</sup> Harmonizált okmánykód, lásd az 1999. április 29-i 1999/37/EK tanácsi irányelvet.

<sup>(3)</sup> Luxemburgban a gépjárművek forgalmi engedélyén két különböző azonosítószám is szerepel.

## 2. Adatbiztonság

### 2.1. Áttekintés

Az Eucaris szoftveralkalmazás a többi tagállammal folytatott biztonságos kommunikációt kezeli, és a tagállamok XML nyelvet alkalmazó back-end kiváltandó rendszereivel (legacy system) kommunikál. A tagállamok üzenetváltáskor az üzenetet közvetlenül a címzettnek küldik. A tagállamok adatközpontja összeköttetésben áll az EU TESTA hálózatával.

A hálózaton keresztül továbbított XML-üzenetek rejtjelezettek. Az üzenetek rejtjelezésére használt technika az SSL adattovábbítási protokoll. A back-end szerverre küldött üzenetek nem rejtjelezett XML-üzenetek, mivel az alkalmazás és a back-end szerver közötti kapcsolatnak védett közegben kell végbemennie.

Egy kliensalkalmazás áll rendelkezésre ahhoz, hogy a tagállamok saját nyilvántartásukban vagy más tagállamok nyilvántartásában keresni tudjanak. Az ügyfelek azonosságát felhasználói azonosító és jelszó vagy klienstanúsítvány révén ellenőrzik. A felhasználókhöz való kapcsolódás rejtjelezhető, de ez az egyes tagállamok felelőssége.

### 2.2. Az üzenetváltással kapcsolatos biztonsági jellemzők

A biztonsági kialakítás alapja a HTTPS- és XML-aláírás kombinációja. Ez a változat XML-aláírást használ a szerver felé küldött valamennyi üzenet aláírására, az üzenet feladóját pedig az aláírás ellenőrzésével hitelesíteni tudja. A továbbított üzenet titkosságának és sértetlenségének megőrzésére egyoldalú SSL-t (csak szervertanúsítvány) használnak, amely védelmet nyújt az üzenet törlésére/visszajátzására és új üzenet beszúrására irányuló támadások ellen. A kétoldalú SSL végrehajtását szolgáló, testreszabott szoftverfejlesztés helyett XML-aláírást alkalmaznak. Az XML-aláírás használata jobban illeszkedik a webszolgáltatások ütemtervéhez, mint a kétoldalú SSL, ezért stratégikusabb.

Az XML-aláírás többféleképpen is kivitelezhető, de a választott megközelítés szerint a „Web Services Security” (WSS) szabvány részeként kell azt alkalmazni. A WSS leírja az XML-aláírás használatának módját. Mivel a WSS a SOAP szabványra épül, ésszerű a lehető legnagyobb mértékben a SOAP szabványhoz igazodni.

### 2.3. Az üzenetváltáshoz nem kapcsolódó biztonsági jellemzők

#### 2.3.1. A felhasználók hitelesítése

Az Eucaris webes alkalmazás felhasználói felhasználónév és jelszó segítségével hitelesítik magukat. Mivel a Windows szabványos hitelesítési eljárásáról van szó, a tagállamok a felhasználók hitelesítésének szintjét szükség esetén klienstanúsítványok alkalmazásával növelhetik.

#### 2.3.2. Felhasználói szerepek

Az Eucaris szoftveralkalmazás több különböző felhasználói szerepet támogat. Minden egyes szolgáltatás-csoporthoz (klaszter) külön hitelesítés tartozik. Például az „Eucaris-szerződés” funkció (kizárólagos) felhasználói esetleg nem használhatják a „Prüm” funkciót. A rendszergazda-szolgáltatások elválnak a normál végfelhasználói szerepektől.

#### 2.3.3. Az üzenetváltás naplózása és visszakereshetősége

Az Eucaris szoftveralkalmazás lehetővé teszi valamennyi üzenettípus naplózását. Egy rendszergazda-funkció lehetővé teszi a nemzeti rendszergazda számára annak meghatározását, hogy mely üzeneteket naplózzák: a végfelhasználók kérelmeit, a többi tagállamtól beérkező kérelmeket, a nemzeti nyilvántartásból szolgáltatott információkat stb.

Az alkalmazás konfigurálható úgy, hogy e naplózás céljára egy belső adatbázist vagy egy külső (Oracle) adatbázist használjon. A naplózandó üzenetekre vonatkozó döntés egyértelműen attól függ, hogy a kiváltandó rendszerekben (legacy system) és a kapcsolt kliensalkalmazásokban máshol milyen naplózási módszert alkalmaznak.

Minden egyes üzenet fejléce információt nyújt a kérelmező tagállamról, e tagállamon belül a kérelmező szervezetről és az érintett felhasználóról. A kérelem indoka is fel van tüntetve.

A kérelmező és a választ adó tagállam általi, kettős naplózás következtében bármely üzenetváltás tökéletesen visszakereshető (például egy érintett állampolgár kérésére).

A naplózás konfigurálása az Eucaris webkliensen keresztül történik (menürendezés, naplózás konfigurálása). A naplózás funkciót a Core System (alaprendszer) hajtja végre. Ha a naplózás aktív, a teljes üzenet (fejléc és levéltest) egyetlen naplóbejegyzésben tárolódik. Meghatározott szolgáltatásokként és az alaprendszeren áthaladó üzenettípusokként beállítható a naplózási szint.

#### Naplózási szintek

Az alábbi naplózási szinteket lehet beállítani:

Privát – üzenet naplózása: A naplózott adatok kinyerését lehetővé tevő szolgáltatás NEM elérhető, az csak nemzeti szinten, audit és problémamegoldás céljából áll rendelkezésre.

Kikapcsolva – az üzenet naplózására nem kerül sor.

#### Üzenettípusok

A tagállamok közötti információcsere többféle üzenetből áll, amelyek sematikus megjelenítése az alábbi ábrán látható.

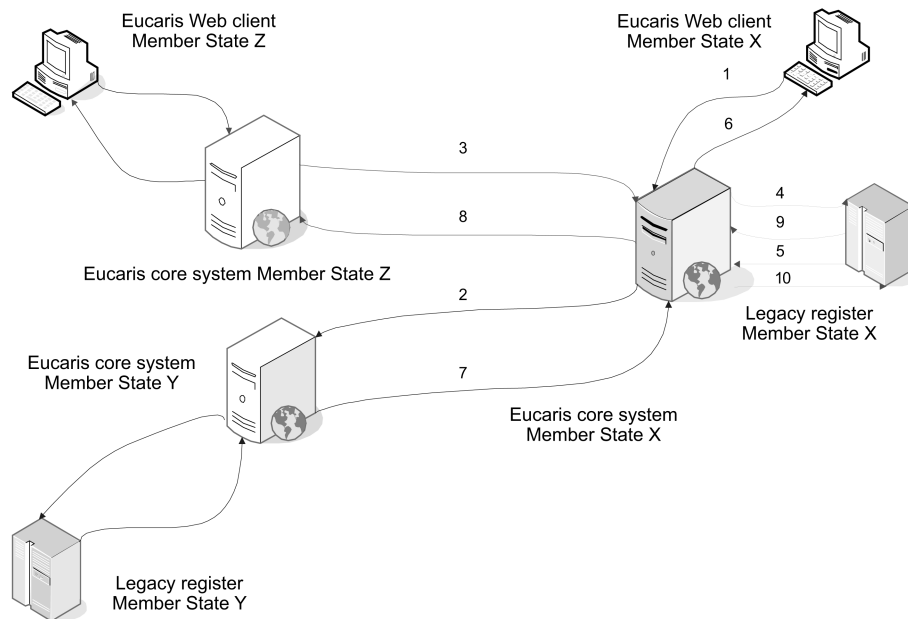
A lehetséges üzenettípusok a következők (az ábrán X tagállam Eucaris alaprendszerére értelmezve):

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

Az ábrán az alábbi információcserek láthatók:

- Információkérés X tagállamtól Y tagállam felé – kék nyilak. Ez a fajta kérés és válasz az 1., 2., 7., illetve 6. üzenettípust foglalja magában.
- Információkérés Z tagállamtól X tagállam felé – piros nyilak. Ez a fajta kérés és válasz a 3., 4., 9., illetve 8. üzenettípust foglalja magában.
- Információkérés a kiváltandó rendszer (legacy system) nyilvántartása felől annak alaprendszere felé (ebbe az útvonalba a kiváltandó rendszer (legacy system) nyilvántartásán túli valamely egyéni kliens kérése is beletartozik) – zöld nyilak. Ez a fajta kérés az 5. és 10. üzenettípust foglalja magában.

Ábra: Naplózási üzenettípusok



#### 2.3.4. Hardver biztonsági modul

Hardver biztonsági modul alkalmazására nem kerül sor.

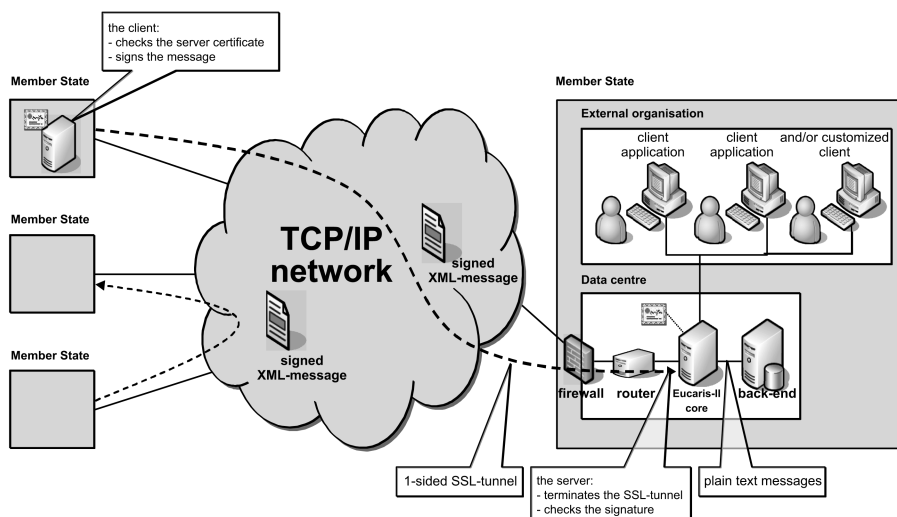
A hardver biztonsági modul (HSM) használata kellő védelmet nyújt az üzenetek aláírására és a szerver azonosítására használt kulcs számára. Ez növeli a biztonság általános szintjét, de a HSM megvétele és fenntartása sokba kerül, és a biztonsági követelmények nem teszik szükségessé FIPS 140-2 2. vagy 3. szintű HSM használatát. Tekintettel arra, hogy az alkalmazott zárt rendszer eredményesen csökkenti a kockázatokat, az a döntés született, hogy kezdetben HSM használatára nem kerül sor. Amennyiben például akkreditáció megszerzéséhez HSM-re van szükség, az beilleszthető az architektúrába.

### 3. Az adatcsere technikai feltételei

#### 3.1. Az Eucaris alkalmazás általános ismertetése

##### 3.1.1. Áttekintés

Az Eucaris alkalmazás valamennyi részt vevő tagállamot szövevényes hálózatban kapcsolja össze, ahol minden egyes tagállam közvetlenül kommunikál a többi tagállammal. A kommunikáció létrehozásához nincs szükség központi elemre. Az Eucaris alkalmazás a többi tagállammal folytatott biztonságos kommunikációt kezeli, és a tagállamok XML nyelvet alkalmazó back-end kiváltandó rendszereivel (legacy system) kommunikál. A struktúrárt az alábbi ábra mutatja be.



A tagállamok üzenetváltáskor az üzenetet közvetlenül a címzettnek küldik. A tagállamok adatközpontja összeköttetésben áll az üzenetváltásra használt hálózattal (TESTA). A tagállamok a nemzeti kapun keresztül csatlakozással férnek hozzá a TESTA hálózathoz. A hálózathoz való csatlakozás során tűzfalat kell használni, és az Eucaris alkalmazásnak hálózati forgalomirányítón (router) keresztül kell a tűzfalhoz kapcsolódnia. Az üzenetek védelmére választott változattól függően vagy az adatútválasztó, vagy az Eucaris alkalmazás tanúsítványt használ.

Egy kliensalkalmazás áll rendelkezésre ahhoz, hogy a tagállamok saját nyilvántartásukban vagy más tagállamok nyilvántartásában keresni tudjanak. A kliensalkalmazás az Eucarishoz kapcsolódik. Az ügyfelek azonosságát felhasználói azonosító és jelszó vagy klienstanúsítvány révén ellenőrzik. A külső szervezetenél (pl. rendőrség) található felhasználókhöz való kapcsolódás rejtjelezhető, de ez az egyes tagállamok felelőssége.

### 3.1.2. A rendszer alkalmazási köre

Az Eucaris rendszer alkalmazási köre a tagállamok jármű-nyilvántartási hatóságai közötti információcseréhez kötődő folyamatokra és ezen információk alapszintű megjelenítésére korlátozódik. Az információ felhasználása során alkalmazandó eljárások és automatizált folyamatok a rendszer alkalmazási körén kívül esnek.

A tagállamok – választásuk szerint – vagy az Eucaris kliens funkciót használják, vagy saját, testreszabott kliensalkalmazást hoznak létre. A lenti táblázat összefoglalja, hogy az Eucaris rendszer mely vonatkozásait kell kötelező jelleggel és/vagy előírás szerint alkalmazni, illetve melyek alkalmazása nem kötelező és/vagy a tagállamok által szabadon meghatározható.

Eucaris aspects	M/O <sup>(1)</sup>	Remark
Network concept	M	The concept is an „any-to-any” communication.
Physical network	M	TESTA
Core application	M	The core application of Eucaris has to be used to connect to the other Member States. The following functionality is offered by the core: <ul style="list-style-type: none"> <li>— Encrypting and signing of the messages;</li> <li>— Checking of the identity of the sender;</li> <li>— Authorization of Member States and local users;</li> <li>— Routing of messages;</li> <li>— Queuing of asynchronous messages if the recipient service is temporarily unavailable;</li> <li>— Multiple country inquiry functionality;</li> <li>— Logging of the exchange of messages;</li> <li>— Storage of incoming messages</li> </ul>
Client application	O	In addition to the core application the Eucaris II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the Eucaris organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the Eucaris organisation and this Council Decision. The specifications can only be changed by the Eucaris organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the Eucaris organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

<sup>(1)</sup> M = kötelező az alkalmazása, illetve betartása, O = nem kötelező az alkalmazása, illetve betartása

3.2. *Funkcionális és nem funkcionális követelmények*3.2.1. *Általános funkciók*

Ez a szakasz általánosan ismerteti a főbb általános funkciókat.

Sorszám	Leírás
1.	A rendszer lehetővé teszi a tagállamok jármű-nyilvántartási hatóságai számára, hogy interaktív módon váltsanak kérelmező és válaszüzeneteket egymással.
2.	A rendszernek része egy kliensalkalmazás, melynek segítségével a végfelhasználók kézi feldolgozásra alkalmas formában küldhetik el kérelmeiket, illetve jeleníthetik meg a válaszinformációkat.
3.	A rendszer lehetővé teszi az üzenetszórást, miáltal egy adott tagállam kérelmét egyszerre az összes többi tagállam felé elküldheti. A beérkező válaszokat az alapalkalmazás összevontan, egyetlen válaszüzenetben küldi el a kliensalkalmazásnak (e funkció neve: „Multiple Country Inquiry”).
4.	A rendszer különböző üzenettípusok kezelésére képes. A felhasználói szerepek, a hitelesítés, az adatútképzés, az aláírás és a naplózás meghatározása szolgáltatásonként külön történik.
5.	A rendszer lehetővé teszi a tagállamok számára a csoportos üzenetküldést, illetve a nagy számú kérelmet vagy választ tartalmazó üzenetek küldését. Az ilyen üzenetek kezelése aszinkron módon történik.
6.	A rendszer sorba állítja és várakoztatja az aszinkron üzeneteket, ha a címzett tagállam átmenetileg nem elérhető, és garantálja a kézbesítést, mielőtt a címzett újra elérhető.
7.	A rendszer a beérkező aszinkron üzeneteket mindaddig tárolja, amíg feldolgozásuk lehetővé nem válik.
8.	A rendszer kizárólag más tagállamok Eucaris alkalmazásai számára biztosítja a hozzáférést, a tagállamokon belül egyéni szervezetek számára nem, vagyis mindegyik jármű-nyilvántartási hivatal egyetlen átjáróként működik a nemzeti végfelhasználók és a többi tagállam megfelelő hatóságai között.
9.	Lehetőség van különböző tagállamok felhasználóinak egy Eucaris szerveren való meghatározására, és a szerveret birtokló tagállam jogai alapján történő hitelesítésükre.
10.	A kérelmező tagállamra, szervezetre és végfelhasználóra vonatkozó információkat az üzenetek tartalmazzák.
11.	A rendszer lehetővé teszi a különböző tagállamok közötti, valamint az alapalkalmazás és a nemzeti nyilvántartási rendszerek közötti üzenetváltás naplózását.
12.	A rendszer lehetővé teszi, hogy egy külön titkár – amely egy kifejezetten erre a feladatra kijelölt szervezet vagy tagállam – a küldött és kapott üzenetekről valamennyi részt vevő tagállam vonatkozásában összegyűjtse a naplózott információkat statisztikai jelentések készítése céljából.
13.	Minden egyes tagállam maga adja meg, hogy a naplózott információk közül melyeket bocsátja a titkár rendelkezésére, illetve hogy mely információk „privát” jellegűek.
14.	A rendszer az egyes tagállamok nemzeti rendszergazdái számára lehetővé teszi felhasználási statisztikák kinyerését.
15.	A rendszerbe egyszerű adminisztratív lépésekkel beléphetnek újabb tagállamok.

3.2.2. *Használhatóság*

Sorszám	Leírás
16.	A rendszer interfészt nyújt az üzenetek back-end rendszerek/kiváltandó rendszerek (legacy system) általi automatizált feldolgozására, és lehetővé teszi a felhasználói felület integrációját ezen rendszerekbe (testreszabott felhasználói felület).
17.	A rendszer könnyen tanulható, magától értetődő és sűgőt tartalmaz.
18.	A rendszer dokumentációja segíti a tagállamokat az integrációban, a működtetésben és a későbbi karbantartásban (pl. kézikönyvek, funkcionális/műszaki dokumentáció, működési útmutató stb.).
19.	A felhasználói felület többnyelvű, és lehetőséget nyújt arra, hogy a végfelhasználó megválassza a használni kívánt nyelvet.
20.	A felhasználói felület tartalmaz olyan eszközöket, amelyek segítségével a helyi rendszergazda a képernyőelemeket és a kódolt információkat is lefordíthatja a nemzeti nyelvre.

## 3.2.3. Megbízhatóság

Sorszám	Leírás
21.	A rendszer szilárd, megbízható operációs rendszer, amely jól tűri a kezelői hibákat, és amely nehézség nélkül helyreáll áramkimaradás vagy egyéb katasztrófa után. A rendszer újraindításának adatvesztés nélkül vagy minimális adatvesztéssel lehetségesnek kell lennie.
22.	A rendszernek stabil, reprodukálható eredményeket kell adnia.
23.	A rendszert úgy alakították ki, hogy az megbízhatóan működjön. A rendszert lehetséges olyan konfigurációban futtatni, amely 98 %-os elérhetőséget garantál (redundanciával, tartalékszerverek használatával stb.) minden egyes kétoldalú kommunikációban.
24.	Lehetséges a rendszer részleges használata, még egyes összetevők meghibásodása alatt is (ha C tagállam leállt, A és B tagállam még tud kommunikálni egymással). Az információfolyamon belüli egyes meghibásodási pontok számát minimalizálni kell.
25.	A súlyos meghibásodást követő helyreállási időnek egy napnál rövidebbnek kell lennie. A leállás ideje távsegítség (pl. egy központi szolgálat) igénybevételével minimálisra csökkenthető.

## 3.2.4. Teljesítmény

Sorszám	Leírás
26.	A rendszer a hét minden napján 24 órában használható. Ezt az időkeretet (24x7) ezért a tagállamok kiváltandó rendszereinek (legacy system) is biztosítaniuk kell.
27.	A rendszer gyorsan válaszol a felhasználói kérelmekre, függetlenül a háttérfeladatoktól. Az elfogadható válaszadási idő biztosítása érdekében ez a felek kiváltandó rendszereitől (legacy system) is elvárt. Az egyes kérelmek esetén általában maximum 10 másodperces válaszadási idő tekinthető elfogadhatónak.
28.	A rendszert többfelhasználós rendszerként alakították ki, úgy, hogy a háttérfeladatok nem szakadnak meg, miközben a felhasználó az aktív feladatokat végzi.
29.	A rendszer méretezhető, ami támogatja annak kezelését, amikor új funkció, új szervezetek vagy tagállamok hozzáadásakor az üzenetek száma – nagy valószínűséggel – megnő.

## 3.2.5. Biztonság

Sorszám	Leírás
30.	A rendszer (pl. biztonsági intézkedései révén) alkalmas olyan üzenetek továbbítására, amelyek „EU restricted” minősítés alá eső, a magánélet védelmét igénylő személyes adatokat tartalmaznak (pl. a gépkocsi tulajdonosára vagy üzemben tartózára vonatkozóan).
31.	A rendszer karbantartása során az adatokhoz való illetéktelen hozzáférés nem lehetséges.
32.	A rendszer a nemzeti végfelhasználók jogait és engedélyeit kezelő szolgáltatást biztosít.
33.	A tagállamok a feladó azonosságát az XML-aláírás révén ellenőrizhetik (tagállami szinten).
34.	A tagállamoknak külön fel kell hatalmazniuk más tagállamokat arra, hogy speciális információkat kérjenek le.
35.	A rendszer az alkalmazás szintjén az ilyen helyzetekben elvárt biztonsági szintnek megfelelő, teljes körű biztonsági és rejtjelezési politikát alkalmaz. Az információ kizárólagosságát és sértetlenségét az XML-aláírás használata garantálja, a rejtjelezést pedig az SSL-alagutazás.
36.	Valamennyi üzenetváltás visszakereshető a naplózás segítségével.
37.	A rendszer védelmet nyújt a törlésre irányuló támadások (egy harmadik fél törli az üzenetet) és a visszajátszásra vagy beszúrásra irányuló támadások (egy harmadik fél visszajátssza az üzenetet vagy beszúr egy üzenetet) ellen.
38.	A rendszer „megbízható harmadik fél” (TTP) tanúsítványokat használ.
39.	A rendszer képes arra, hogy egyazon tagállam vonatkozásában – az üzenet vagy szolgáltatás típusától függően – különféle tanúsítványokat vegyen figyelembe.

Sorszám	Leírás
40.	Az alkalmazás szintű biztonsági intézkedések elegendőek a nem akkreditált hálózatok igénybevételének engedélyezéséhez.
41.	A rendszer képes az olyan újabb biztonsági technikák alkalmazására, mint például az XML-tűzfal.

## 3.2.6. Alkalmazkodóképesség

Sorszám	Leírás
42.	A rendszer új üzenetekkel és új funkciókkal bővíthető. A kiigazítás költségei elhanyagolhatók. Ez annak köszönhető, hogy az alkalmazás elemeit központilag fejlesztik.
43.	A tagállamok kétoldalú alkalmazás céljára új üzenettípusokat határozhatnak meg. Nem szükséges, hogy minden tagállam minden típusú üzenetet támogasson.

## 3.2.7. Támogatás és karbantartás

Sorszám	Leírás
44.	A rendszer egy központi szolgálat és/vagy operátorok számára felügyeleti eszközöket biztosít a hálózat és a különböző tagállamokban működő szerverek felett.
45.	A rendszer lehetőséget nyújt a központi szolgálat részéről nyújtott távsegítségre.
46.	A rendszer lehetőséget nyújt problémaelemzésre.
47.	A rendszer kiterjeszhető új tagállamokra.
48.	Az alkalmazás telepítése alapszintű informatikai képzettséggel és tapasztalattal rendelkező személyzet számára is egyszerű feladat. A telepítési eljárásnak a lehető legnagyobb mértékben automatikusan kell lefutnia.
49.	A rendszer állandó tesztelési és elfogadási környezetet biztosít.
50.	Az éves karbantartási és támogatási költségeket minimálisra csökkentették azáltal, hogy igazodtak a piaci szabványokhoz, valamint úgy alakították ki az alkalmazást, hogy a központi szolgálat segítségét minél kevesebb esetben kelljen igénybe venni.

## 3.2.8. Tervezési követelmények

Sorszám	Leírás
51.	A rendszer működési élettartama – kialakítása és dokumentációja alapján – hosszú éveket ölel fel.
52.	A rendszer független a hálózatszolgáltatótól.
53.	A rendszer alkalmazkodik a tagállamok meglévő hardvereihez és szoftvereihez azáltal, hogy azok nyilvántartási rendszereivel nyílt szabványon alapuló webszolgáltatási technológiák segítségével kommunikál (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 stb.).

## 3.2.9. Alkalmazandó szabványok

Sorszám	Leírás
54.	A rendszer megfelel a 45/2001/EK rendeletben (21., 22. és 23. cikk) és a 95/46/EK irányelvben meghatározott adatvédelmi előírásoknak.
55.	A rendszer megfelel az IDA szabványoknak.
56.	A rendszer támogatja az UTF8 kódolást.

#### 4. FEJEZET: **Értékelés**

##### 1. **A 20. cikk szerinti értékelési eljárás (a 2008/615/IB határozat 25. cikkének (2) bekezdése szerinti határozatok előkészítése)**

###### 1.1. *Kérdőív*

Az érintett tanácsi munkacsoportok kérdőívet állítanak össze a 2008/615/IB határozat 2. fejezetében meghatározott valamennyi automatizált adatcserét illetően.

Amint egy tagállam úgy véli, hogy egy adott adatkategória tekintetében teljesíti az adatcsere előfeltételeit, kitölti a megfelelő kérdőívet.

###### 1.2. *Kísérleti adatcsere*

A kérdőív eredményeinek értékelése céljából az adatcserét megkezdni szándékozó tagállam kísérleti adatcserét végez egy vagy több másik, a tanácsi határozat alapján már adatcserét folytató tagállammal együtt. A kísérleti adatcsere röviddel az értékelő látogatás előtt vagy után kerül sor.

A kísérleti adatcsere feltételeit és szabályait a megfelelő tanácsi munkacsoport határozza majd meg az érintett tagállammal előzetesen kötött egyéni megállapodás alapján. A gyakorlati részletekről a kísérleti adatcsereben részt vevő tagállamok maguk határozzák.

###### 1.3. *Értékelő látogatás*

A kérdőív eredményeinek értékelése céljából az adatcserét megkezdni szándékozó tagállamban értékelő látogatásra kerül sor.

E látogatás feltételeit és szervezési kérdéseit a megfelelő munkacsoport határozza majd meg az érintett tagállam és az értékelő csoport közötti előzetes, egyéni megállapodás alapján. Az érintett tagállam lehetővé teszi az értékelő csoport számára, hogy az értékelendő adatkategóriába vagy -kategóriákba tartozó adatok automatizált cseréjét ellenőrizze, különösen azáltal, hogy az értékelő csoport kéréseinek figyelembevételével szervezi meg a látogatás programját.

Az értékelő csoport az értékelő látogatásról egy hónapon belül jelentést készít, és észrevételezés céljából továbbítja azt az érintett tagállamnak. Adott esetben az értékelő csoport a tagállam észrevételei alapján felülvizsgálja a jelentést.

Az értékelő csoport legfeljebb három szakértőből áll, akiket az értékelendő adatkategóriákon belül automatizált adatcserét folytató tagállamok jelölnek ki, akik tapasztalattal rendelkeznek az érintett adatkategóriát illetően, megfelelő nemzetbiztonsági átvilágításon estek át, mely alapján foglalkozhatnak e kérdésekkel, valamint készek részt venni egy másik tagállamban legalább egy értékelő látogatáson. A Bizottság felkérést kap, hogy megfigyelőként csatlakozzon az értékelő csoporthoz.

Az értékelő csoport tagjai tiszteletben tartják, hogy a feladatuk ellátása során szerzett információk bizalmas jellegűek.

###### 1.4. *Jelentés a Tanácsnak*

A kérdőívek, az értékelő látogatás és a kísérleti adatcsere eredményeit összegző, általános értékelő jelentés készül a Tanács részére, melynek alapján az meghozhatja a 2008/615/IB határozat 25. cikkének (2) bekezdése szerinti határozatát.

##### 2. **A 21. cikk szerinti értékelési eljárás**

###### 2.1. *Statisztika és jelentés*

Minden egyes tagállam statisztikát készít az automatizált adatcsere eredményeiről. Az összehasonlíthatóság érdekében az érintett tanácsi munkacsoport összeállít egy mintastatisztikát.

Ezeket a statisztikákat évente kell továbbítani a Főtitkárságnak – amely összegző áttekintést készít az elmúlt évről –, valamint a Bizottságnak.

Ezenkívül a tagállamok felkérést kapnak, hogy rendszeres időközönként, évente legfeljebb egyszer a folyamat elemzése és fejlesztése érdekében nyújtsanak további információkat – szükség szerint – az automatizált adatcsere megvalósításának adminisztratív, technikai és pénzügyi vonatkozásairól. Ezen információk alapján jelentés készül a Tanács részére.



2.2. *Felülvizsgálat*

A Tanács – ésszerű határidőn belül – tanulmányozza a fent ismertetett értékelési mechanizmusokat, és szükség esetén felülvizsgálja azokat.

3. Szakértői értekezletek

A szakértők az érintett tanácsi munkacsoport keretében rendszeresen összeülnek annak érdekében, hogy megszervezzék és elvégezzék a fent említett értékelési eljárásokat, valamint megosszák egymással tapasztalataikat és megvitassák az esetlegesen szükséges javító lépéseket. Adott esetben e szakértői megbeszélések eredményeit beépítik a 2.1. pontban említett jelentésbe.

---

## A TANÁCS 2008/617/IB HATÁROZATA

(2008. június 23.)

az Európai Unió tagállamainak különleges intervenciók egységei közötti együttműködés javításáról  
válsághelyzetekben

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unióról szóló szerződésre és különösen annak 30. cikkére, 32. cikkére, valamint 34. cikke (2) bekezdésének c) pontjára,

tekintettel az Osztrák Köztársaság kezdeményezésére <sup>(1)</sup>,

tekintettel az Európai Parlament véleményére <sup>(2)</sup>,

mivel:

- (1) A Szerződés 29. cikke kimondja, hogy az Unió célja, hogy a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés területén a tagállamok közös fellépésének kidolgozásával biztosítsa a polgárok magas szintű biztonságát egy olyan térségben, amely a szabadságon, a biztonságon és a jog érvényesülésén alapul.
- (2) Az Európai Unió tagállamainak állam- és kormányfői 2004. március 25-i, a terrorizmus elleni szolidaritási nyilatkozatukban kinyilvánították azon határozott szándékukat, hogy a tagállamok minden rendelkezésükre álló eszközt mozgósítsanak annak érdekében, hogy terrorista támadás esetén az érintett tagállamnak vagy csatlakozó államnak – politikai hatóságai kérésére – saját területén segítséget nyújtsanak.
- (3) A 2001. szeptember 11-i támadásokat követően a rendőrségi vezetők munkacsoportjának égisze alatt megindult az együttműködés a tagállamok valamennyi bűnüldöző hatóságának különleges intervenciók egységei között. „Atlasz” elnevezésű hálózatuk 2001 óta számos szemináriumot tartott, tanulmányt készített, tárgyi cserét és közös gyakorlatot hajtott végre.
- (4) Egyetlen tagállam sem rendelkezik a lehetséges, különleges beavatkozást igénylő, különleges vagy nagy horderejű válsághelyzetek hatékony kezeléséhez szükséges valamennyi eszközzel, erőforrással és szakértelemmel. Különös jelentősége van ezért annak, hogy minden tagállam kérhesse más tagállamok segítségét.
- (5) A különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló, 2008. június 23-i 2008/615/IB tanácsi határozat <sup>(3)</sup> („prümi határozat”) és különösen annak 18. cikke szabályozza a nagy tömegeket vonzó eseményekkel és hasonló nagyszabású eseményekkel,

valamint katasztrófákkal és súlyos balesetekkel kapcsolatos, tagállamok közötti rendőrségi segítségnyújtás formáit. Ez a határozat nem terjed ki a prümi határozat 18. cikkében meghatározott nagy tömegeket vonzó eseményekre, természeti katasztrófákra vagy súlyos balesetekre, de kiegészíti a prümi határozatnak a tagállamok közötti, egyéb helyzetekre – azaz személyekre, vagyontárgyakra, infrastruktúrára vagy intézményekre súlyos, közvetlen fizikai fenyegetést jelentő, ember által előidézett válsághelyzetekre, a különösen túszejtésre, repülőgép-eltérítésre és hasonló eseményekre – vonatkozó, különleges intervenciók egységei által történő rendőrségi segítségnyújtás formáit előirányzó rendelkezéseit.

- (6) Ezen jogi keret és az illetékes hatóságokat feltüntetett összeállítás rendelkezésre állásával a tagállamok egy ilyen válsághelyzet esetén gyorsan reagálhatnak és időt takaríthatnak meg. Ezenkívül a tagállamoknak az ilyen válsághelyzetek és különösen a terrorcselekmények megelőzésére vonatkozó képességének és az azokra való reagálási képességének a megerősítése céljából alapvető fontosságú, hogy a különleges intervenciók egységei rendszeresen találkozzanak és közös képzéseket szervezzenek a kölcsönös tapasztalatok hasznosítása érdekében,

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

1. cikk

Tárgy

Ez a határozat általános szabályokat és feltételeket állapít meg annak céljából, hogy egy adott tagállam különleges intervenciók egységei segítséget nyújthassanak és/vagy műveletet hajthassanak végre egy másik tagállam (a továbbiakban: a megkereső tagállam) területén abban az esetben, ha a megkereső tagállam erre az egységeket felkérte, azok pedig hozzájárultak ehhez valamely válsághelyzet megoldása érdekében. A megkereső tagállam és a megkeresett tagállam az e határozatot kiegészítő gyakorlati részletekről és végrehajtási rendelkezésekről közvetlenül állapodik meg.

2. cikk

### Fogalommeghatározások

E határozat alkalmazásában:

- a) „különleges intervenciók egység”: egy tagállam bármely olyan bűnüldöző egysége, amelynek szakterülete a válsághelyzetek kezelése;

<sup>(1)</sup> HL C 321., 2006.12.29., 45. o.

<sup>(2)</sup> A 2008. január 31-i vélemény (a Hivatalos Lapban még nem tették közzé).

<sup>(3)</sup> Lásd e Hivatalos Lap 1. oldalát.

- b) „válsághelyzet”: bármely olyan helyzet, amikor egy tagállam illetékes hatóságai joggal feltételezik, hogy egy bűncselekmény súlyos, közvetlen fizikai fenyegetést jelent az érintett tagállamban tartózkodó személyekre, az ott található vagyontárgyakra, infrastruktúrára vagy intézményekre, különösen pedig a terrorizmus elleni küzdelemlről szóló, 2002. június 13-i 2002/475/IB tanácsi kerethatározat<sup>(1)</sup> 1. cikkének (1) bekezdésében említett helyzetek;
- c) „illetékes hatóság”: az a nemzeti hatóság, amely kérheti a különleges intervenció egységek bevetését, illetve engedélyt adhat arra.

## 3. cikk

**Segítségnyújtás más tagállam részére**

(1) Az illetékes hatóságokhoz intézett – a segítség jellegét, valamint az ebből következő műveleti szükségleteket meghatározó – kérésben a tagállamok kérhetik, hogy valamely válsághelyzet megoldása érdekében igénybe vehessék egy másik tagállam különleges intervenció egységeinek segítségét. A megkeresett tagállam illetékes hatósága e kérést elfogadhatja vagy elutasíthatja, vagy más jellegű segítséget ajánlhat fel.

(2) Az érintett tagállamok közötti megállapodás függvényében a segítségnyújtás állhat abból, hogy a megkeresett tagállam felszereléssel és/vagy szakértőkkel segíti a megkereső tagállamot, és/vagy annak területén műveletet hajt végre, szükség esetén fegyvereket használva.

(3) A megkereső tagállam területén végrehajtott műveletek esetén a segítséget nyújtó különleges intervenció egység tisztviselői jogosultak arra, hogy a megkereső tagállam területén támogatói minőségben járjanak el és meghozzanak a kért segítség megadásához szükséges minden intézkedést, amennyiben:

- a) tevékenységüket a megkereső tagállam felelőssége, felügyelete és irányítása mellett végzik, a megkereső tagállam jogával összhangban; és
- b) a saját nemzeti joguk szerinti hatáskörük keretein belül járnak el.

## 4. cikk

**Polgári jogi és büntetőjogi felelősség**

Amikor e határozat keretében egy tagállam tisztviselői egy másik tagállamon belül működnek és/vagy felszerelés használatára kerül sor, a prúmi határozat 21. cikke (4) és (5) bekezdésében, valamint 22. cikkében megállapított, polgári jogi és büntetőjogi felelősségre vonatkozó rendelkezéseket kell alkalmazni.

<sup>(1)</sup> HL L 164., 2002.6.22., 3. o.

## 5. cikk

**Találkozók és közös képzések**

A részt vevő tagállamok biztosítják, hogy különleges intervenció egységeik – amennyiben szükséges – találkozókat tartsanak és közös képzéseket és gyakorlatokat szervezzenek abból a célból, hogy megosszák egymással a válsághelyzetek kezelésére vonatkozó tapasztalataikat, szakértelmüket, valamint általános, gyakorlati és technikai jellegű információkat. E találkozók, képzések és gyakorlatok finanszírozhatók az Unió pénzügyi programjai által – az Európai Unió költségvetési támogatásából való részesülés céljára – kínált lehetőségek keretében. Ebben az összefüggésben az Unió elnökségét betöltő tagállam törekszik annak biztosítására, hogy sor kerüljön ilyen találkozókra, képzésekre és gyakorlatokra.

## 6. cikk

**Költségek**

Az érintett tagállamok közötti eltérő megállapodás hiányában a megkereső tagállam viseli a megkeresett tagállam különleges intervenció egységeinek a 3. cikk alkalmazásával kapcsolatosan felmerülő műveleti költségeit, beleértve a szállítási és szállásköltségeket.

## 7. cikk

**Más jogi eszközökkel való kapcsolat**

(1) A Szerződés VI. címe alapján elfogadott egyéb aktusokban, különösen a prúmi határozatban vállalt kötelezettségeik sérelme nélkül:

- a) A tagállamok továbbra is alkalmazhatják a határokon átnyúló együttműködésre vonatkozó, 2008. június 23-án hatályban lévő két- vagy többoldalú megállapodásokat vagy szabályozásokat, amennyiben e megállapodások vagy szabályozások nem összeegyeztethetetlenek e határozat célkitűzéseivel.
- b) A tagállamok 2008. december 23. után köthetnek vagy hatályba léptethetnek a határokon átnyúló együttműködésre vonatkozó két- vagy többoldalú megállapodásokat vagy szabályozásokat, amennyiben ezek rendelkeznek e határozat céljainak kiterjesztéséről vagy kibővítéséről.

(2) Az (1) bekezdésben említett megállapodások és szabályozások nem érinthetik az e megállapodásokban és megegyezésekben nem részes tagállamokkal fennálló kapcsolatokat.

(3) A tagállamok az (1) bekezdésben említett megállapodásokról vagy szabályozásokról tájékoztatják a Tanácsot és a Bizottságot.

## 8. cikk

**Záró rendelkezések**

A Tanács Főtitkársága összeállítja és naprakészen tartja a tagállamok azon illetékes hatóságainak jegyzékét, amelyek a 3. cikk szerinti segítséget kérhetnek és segítségnyújtásra engedélyt adhatnak.

A Tanács Főtitkársága tájékoztatja az (1) bekezdésben említett hatóságokat az e cikk szerint összeállított jegyzéket érintő valamennyi változásról.

## 9. cikk

**Hatálybalépés**

Ez a határozat 2008. december 23-án lép hatályba.

Kelt Luxembourgban, 2008. június 23-án.

*a Tanács részéről*

*az elnök*

I. JARC

---