MAGYAR KÖZLÖNY

A MAGYAR KÖZTÁRSASÁG HIVATALOS LAPJA

Budapest,
2007. október 31.,
szerda

147. szám

II. kötet

Ára: 3000,– Ft

TARTALOMJEGYZÉK

A Kormány 288/2007. (X. 31.) Korm. rendelete

a Prümi Szerződésben meghatározott Nyilatkozatok megtételéről, valamint a Prümi Szerződés Adminisztratív és Technikai Végrehajtási Megállapodásának kihirdetéséről

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 a határon átnyúló együttműködés fokozásáról, különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció leküzdése érdekében létrejött Szerződés (Prümi Szerződés) kihirdetéséről szóló 2007. évi CXII. törvény 12. §-ában kapott felhatalmazás alapján a Kormány kihirdeti a következő Nyilatkozatokat:

„A Magyar Köztársaság Kormánya a következőkről értesíti a Németországi Szövetségi Köztársaság Kormányát, mint a Prümi Szerződés letéteményesét:

a) a Prümi Szerződés 6. Cikk 1. bekezdésében, 11. Cikk 1. bekezdésében és 12. Cikk 2. bekezdésében említett nemzeti kapcsolattartó pont a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala;

b) a Prümi Szerződés 15. Cikkében, 16. Cikk 3. bekezdésében és 19. Cikkében említett nemzeti kapcsolattartó pont az Országos Rendőr-főkapitányság;

c) a Prümi Szerződés 22. Cikkében említett nemzeti kapcsolattartó pont a Határőrség Országos Parancsnoksága;

d) a Prümi Szerződés 23. Cikk 3. bekezdésében említett nemzeti kapcsolattartó pont a Bevándorlási és Állampolgársági Hivatal;

e) a Prümi Szerződés 24–27. Cikkeiben említett hatáskörrel rendelkező hatóságok és tisztségviselők alatt a Rendőrséget és a Vám- és Pénzügyőrséget, illetve a Rendőrség és a Vám- és Pénzügyőrség állományába tartozó személyeket kell érteni.”

2. §

A Kormány a Prümi Szerződés 44. Cikke alapján 2006. december 5-én, Brüsszelben létrejött Adminisztratív és Technikai Végrehajtási Megállapodást e rendelettel kihirdeti.

3. §

Az Adminisztratív és Technikai Végrehajtási Megállapodás hiteles szövege és annak hivatalos magyar fordítása a következő:

„Implementing Agreement

of the Treaty between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed in Prüm, Germany, on 27 May 2005.

Section 1: Scope and definitions

1. Scope

According to article 44 of the Treaty, the scope of this Implementing Agreement is to decide the necessary provisions for the administrative and technical implementation and application of the Treaty.

2. Definitions

For the purpose of this Implementing Agreement:

2.1 "Treaty" means the Treaty between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed in Prüm, Germany, on 27 May 2005;

2.2 "Party" means a Contracting Party of the Treaty which has signed the present Implementing Agreement;

2.3 the procedures of "search", "comparison" or "searches by comparing" as referred to in articles 3, 4 and 9 of the Treaty means the procedures by which it is established whether there is a match between respectively DNA data or dactyloscopic data, which has been communicated by one Party, with the DNA data or the dactyloscopic data stored in the data bases of one, more, or all of the other Parties;

2.4 "DNA profile" means a letter or a number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular chemical form at the various DNA locations (loci);

2.5 "non-coding part of DNA" means chromosome zones containing no genetic expression, i.e. not known to provide information about specific hereditary characteristics;

2.6 "DNA reference data" means a DNA profile and the linked non DNA specific data;

2.7 "non DNA specific data" comprises:

2.7.1 an identification code or number allowing, in case of a match, the Parties to retrieve personal data and / or other information in their databases in order to supply it to one, more or all of the other Parties, pursuant to article 5 of the Treaty;

2.7.2 a Party code to indicate the national origin of the DNA profile, and

2.7.3 a code to indicate the type of DNA profile as declared by the Parties according to article 2 paragraph 2 of the Treaty;

2.8 “unidentified DNA profile” means the DNA profile obtained from stains stemming from the investigation of criminal offences and belonging to a not yet identified person;

2.9 “reference DNA profile“ is used as a technical expression and means the DNA profile of an identified person included in the national DNA analysis files according to article 2 paragraph 3 of the Treaty;

2.10 “dactyloscopic data” means fingerprint images, images of fingerprint latents, palm prints, palm print latents as well as templates of such images (*minutiae*), as far as they are stored and dealt with in an automated database;

2.11 “follow-up request” means the request addressed by one Party to one, more or all of the other Parties in case of a match of compared DNA or dactyloscopic data, in order to obtain further personal data and other information according to articles 5 and 10 of the Treaty;

2.12 “vehicle registration data” means the data-set as specified in Annex C.1 on which the Parties agreed to make them mutually available for an automated search procedure as defined in point 2.13 hereafter;

2.13 “automated searching” means an online access procedure in order to consult, in accordance with article 33 paragraph 1, point 2 of the Treaty, the databases of one, more or all of the other Parties;

2.14 “the system ex article 12” means all technical measures and functional aspects, such as network, interfaces and security issues, established for the exchange of vehicle register data according to article 12 of the Treaty;

2.15 “EUCARIS” means the European Vehicle and Driving License Information System as established by the relevant Treaty, signed in Luxembourg on the 29th June 2000;

2.16 “individual cases”, as referred to in article 3 paragraph 1, article 9 paragraph 1 and article 12 paragraph 1 of the Treaty, means one single investigation or prosecution file; if such a file contains more than one DNA profile, dactyloscopic data or vehicle register data, they may be, respectively, transmitted together as one search query;

2.17 “reason for search or supply of data” means for the application of article 39 of the Treaty, an indication which enables to establish a clear link between a particular request and the corresponding individual case which gave rise to the request;

2.18 “TESTA II communication network” means the “Trans European Services for Telematics between Administrations” managed by the European Commission, as well as any modified version of it.

Section 2: DNA profiles

3. Composition and comparison of DNA profiles

3.1 For the purpose of the implementation of article 2 of the Treaty, the DNA reference data which are to be exchanged under the terms of the Treaty are composed of a DNA profile and the non DNA specific data.

3.2 A set of common technical specifications, including matching rules, algorithms and Parties code numbers, as defined in Annexes A, will be implemented and deployed at the national contact points of the Parties and will be applied to all queries and answers related to searches and comparisons of DNA profiles, as referred to in point 3.1.

3.3 DNA profiles will be compared on the basis of shared markers as defined in Annex A.1. Any DNA profile transmitted for automated search or comparison by the requesting Party will be compared with any DNA profile made available by the requested Parties pursuant to article 2 paragraphs 2 and 3 of the Treaty.

3.4 The Parties make use of existing standards such as the European Standard Set (ESS) or the Interpol Standard Set of Loci (ISSOL).

4. DNA requesting and reporting rules

4.1 The query for an automated search or comparison, as referred to in articles 3 and 4 of the Treaty, solely includes the following information:

4.1.1 the Party code of the requesting Party;

4.1.2 the date, the time and the reference number of the query;

4.1.3 the DNA profiles and their non DNA specific data;

4.1.4 the type of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles).

4.2 The Parties do the necessary so that queries are in full compliance with the conditions imposed by the declarations referred to article 2 paragraph 3 of the Treaty and reproduced in Annex A.3.

4.3 The answer (matching report) to the query referred to in point 4.1 will be sent to the national contact point of the requesting Party in order to determine if a follow-up request may be made. A matching report contains solely the following information:

4.3.1 the indication whether there was one or more matches (hit) or not (no hit);

4.3.2 the date, the time and the reference number of the query;

4.3.3 the date, the time and the reference number of the answer;

4.3.4 the Party code of the requested Party;

4.3.5 the non DNA specific data of the requesting and the requested Party;

4.3.6 the type of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles);

4.3.7 in the case of a comparison according to article 4 of the Treaty, the matched DNA profile.

4.4 Automated notification of a hit is only provided on condition that the automated search or comparison has resulted in a match of a minimum of loci as set out in Annex A.1. In the case of a searching according to article 3 of the Treaty, for verification purposes, national contact points of the Parties shall take appropriate measures in compliance with their national law.

5. Communication network for transmission of DNA data

The electronic exchange of DNA related data amongst the Parties are deployed by the use of the "TESTA II" communication network according to the technical specifications as set out in Annex A.5.

6. Quality control measures

The Parties take appropriate measures to guarantee the integrity of the DNA profiles made available to the other Parties or transmitted for comparison. These measures shall be in compliance with international standards, such as ISO 17025. The forensic aspects of these DNA profiles have to comply with the specifications set forth in Annex A.1.

Section 3: Dactyloscopic data

7. Transmission of dactyloscopic data

7.1 For the purpose of the implementation of article 9 of the Treaty, the Parties establish a mutually accessible technical entry to their "automated fingerprint identification systems" (called hereafter "AFIS").

7.2 The systems mentioned in point 7.1 only include automated dactyloscopic identification systems established for the prevention and investigation of criminal offences. Data from administrative files must not be transmitted.

7.3 The digitalisation of dactyloscopic data and its transmission to other Parties is carried out according to the data format specified in the "Interface Control Document (ICD)" as defined in Annex B.1. Each Party ensures that the dactyloscopic data transmitted by the other Parties can be compared with the reference data of its own AFIS.

7.4 The references as referred to in article 9 of the Treaty allow the univocal correspondence to a person or a criminal case, as well as the identification of the requesting Party.

8. Search and transmission of results

8.1 The Parties ensure that the transmitted dactyloscopic data is of a suitable quality for a comparison by AFIS. The requested Party checks the quality of the transmitted dactyloscopic data without delay by a fully automated procedure. In case of data being not suitable for an automated comparison, the requested Party informs the requesting Party without delay.

8.2 The requested Party conducts the searches in the order in which requests were received. Requests have to be processed within 24 hours by a fully automated procedure. The requesting Party may, if its national law so demands, ask for an accelerated processing of these searches. The requested Party conducts these searches without delay. If deadlines cannot be met for reasons the requested Party is not responsible, the comparison need to be carried out without delay as soon as the impediments have been removed.

8.3 The requested Party takes care that the system is able to transmit in a fully automated way any hit or no-hit without delay to the requesting Party. In case of a hit, it transmits the dactyloscopic data and the references referred to in article 9 paragraph 2 of the Treaty for all matches between dactyloscopic data.

9. Communication network for transmission of dactyloscopic data

The electronic exchange of dactyloscopic related data between the Parties have to be executed by the use of the "TESTA II" communication network, according to the technical specifications as set out in Annex A.5.

10. Definition and capacities of automated searching of dactyloscopic data

10.1 The maximum amount of the different types of dactyloscopic data (candidates) accepted for verification per transmission is set out in Annex B.2.

10.2 The maximum research capacities per day for dactyloscopic data of identified persons of each Party are set out in Annex B.3.

10.3 The maximum research capacities per day for dactyloscopic traces of each Party are set out in Annex B.4.

Section 4: Vehicle registration data

11. Search procedure and transmission of data

11.1 For the purpose of article 12 of the Treaty, the Parties set up a network of national contact points in order to conduct automated searches in their respective vehicle registration data bases. The technical conditions of the data exchange are set out in Annex C.3.

11.2 Without prejudice to the Treaty's provisions, and taking into account specifically the provisions of articles 38 and 39, the Parties, acting respectively as requesting or requested Party, organise the mode of operation of their national contact points, in good faith to the Treaty's provisions and principles.

11.3 The Parties opting for an entirely automated requesting procedure have to assure that all their requests have to pass through their national contact point provided for by the Treaty, which has to be under the supervision of a responsible officer.

12. Communication network for transmission of vehicle registration data

12.1 As a means for the electronic exchange of vehicle registration data, the Parties decide to use the "TESTA II" communication network and a for the purposes of the system ex article 12 especially designed EUCARIS software application, as well as any modified version of both systems.

12.2 All costs to be shared emanating from the management and the use of the system ex article 12, including the costs related to the EUCARIS technology, have to be discussed and agreed upon on an annual basis.

13. Technical and organisational measures to protect personal data and data security

The technical specifications of the automated search, as referred to in article 38 paragraph 2 of the Treaty, concerning data protection, security, confidentiality and integrity, the network encryption and authorisation procedures as well as the checking procedures for the admissibility of automated searches are detailed in Annex C.2.

Section 5: Police cooperation

14. Joint operations

14.1 By mission statement, two or more Parties may set up a joint operation as referred to in article 24 of the Treaty. Before the start of the operation, they make written or verbal arrangements about the operational modalities, such as:

a) the competent authorities of the Parties to the mission statement;
b) the specific purpose of the operation;
c) the host State where the operation takes place;
d) the geographical area of the host State where the operation takes place;
e) the period covered by the operation mission statement;
f) the specific assistance to be provided by the seconding State to the host State, including officers or other officials, material and financial elements;
g) the officers participating in the operation;
h) the officer who will be in charge of the operation;
i) the powers the officers and other officials of the seconding State may exercise in the host Party during the operation;
j) the particular arms, ammunition and equipment the seconding officers may use during the operation in accordance to the rules laid out in Annex D.3;
k) the logistic modalities concerning transport, accommodation and security;
l) the bearing of costs of the joint operation if it differs from the provision of article 46 of the Treaty;
m) any other possible elements required.

14.2 Bármely Fél kompetens hatósága kezdeményezheti egy közös művelet elindítását. A D.1. Mellékletben bármely Fél rögzítheti a beérkező kérések feldolgozására vonatkozó eljárást. Ha nincs rögzített eljárás, a D.1. Melléklet szerint kijelölt nemzeti kapcsolattartó pont nyújt segítséget a többi Félnek, hogy kérésüket a kompetens hatósághoz juttathassák el.

15. Cross-border operations in the event of imminent danger

15.1. The authorities to be notified without delay, as stipulated in article 25 paragraph 3 of the Treaty, are set out in Annex D.2.

15.2 Any modification of the contact details of these authorities is communicated as soon as possible to the contact points of the other Parties listed also in Annex D.2.

16. The carrying and use of arms, ammunition and equipment

In Annex D.3, each Party lists the particular arms, ammunition and equipment which are prohibited to be carried, according to article 28 paragraph 1, 3rd phrase of the Treaty, the particular arms, ammunition and equipment which are prohibited to be used and the legal aspects according to article 28 paragraph 2 of the Treaty, as well as the practical aspects according to article 28 paragraph 5 of the Treaty.

Section 6: General provisions

17. Evaluation of the application and the implementation of the Treaty and the Implementing Agreement

17.1 The evaluation of the administrative and technical application and implementation of the Treaty and the Implementing Agreement is executed by the Joint Working Group as provided for in article 43 paragraph 2 of the Treaty, or by any specific technical working group mandated for this purpose by the Joint Working Group. Such an evaluation may be executed at the request of any of the Parties.

17.2 The modalities of the automated searching and comparison of DNA and dactyloscopic data will be evaluated, unless otherwise decided upon by the Joint Working Group, six months after the beginning with activities on the basis of this Implementing Agreement. For vehicle registration data, this first evaluation will take place three months after the beginning with activities. Subsequently, such evaluations may take place at the request of any Party according to article 43 of the Treaty.

17.3 The bodies responsible for recording under article 39 paragraph 2 of the Treaty shall carry out random checks in such a frequency and to the extent necessary to ensure an effective evaluation of the lawfulness of automated searches carried out according to articles 3, 9 and 12 of the Treaty by the respective foreign contact points.

18. Availability of automated data exchange

The Parties provide all reasonable efforts to maintain upright the automated on-line exchange of DNA, dactyloscopic and vehicle register data on the basis of a 24 hours per day and 7 days per week availability. In case of a technical failure, the relevant contact points of the Parties inform each other as soon as possible and agree upon a temporary alternative mean of communication, according to any other applicable legal instrument. The automated exchange of data has to be restored as quickly as possible.

19. Modification of the Implementing Agreement and its Annexes

19.1 Modifications to this Implementing Agreement and its Annexes may be proposed by any Party. Such proposals are communicated to all other Parties.

19.2 If the proposed modification relates to the provisions of the Implementing Agreement, it is adopted by a Decision of the Committee of Ministers according to article 43 paragraph 1 of the Treaty.

19.3 If the proposed modification relates to one or more of the Annexes of the Implementing Agreement, it is adopted by the Joint Working Group provided for in article 43 paragraph 2 of the Treaty.

19.4 For the purpose of the modification of this Implementing Agreement or its Annexes, unanimity is reached when the attendant and represented Parties agree on the proposed modification. Consequently, absent and not represented Parties do not prevent the adoption of a modification of the Implementing Agreement. Such a modification applies to all Parties.

20. Taking effect; Signing; Depositary

20.1 For the Parties for which the Treaty entered into force, this Implementing Agreement takes effect after its signature, as well as the adoption of the necessary Decisions provided for in article 34 paragraph 2 of the Treaty. For the other Parties, it will take effect according to article 50 paragraph 1, respectively article 51 paragraph 1, of the Treaty and after the adoption of the necessary Decisions provided for in article 34 paragraph 2 of the Treaty.

20.2 This Implementing Agreement, with its Annexes, will be signed in the German, Spanish, French, Dutch and English languages, which are all equally authentic.

20.3 The Government of the Federal Republic of Germany acts as depositary for this Implementing Agreement and its Annexes.

(Signatures)

List of Annexes

Annexes A: ***Automated searching for DNA-profiles***

Annex A.1 DNA related Forensic Issues, Matching rules and Algorithms [FIMA]

Annex A.2 Party Code Number Table [PCNT]

Annex A.3 Functional Process and Workflow Analysis [FPWA]

Annex A.4 DNA Interface Control Document [DICD]

Annex A.5 Application, Security and Communication Architecture [ASCA]

Annexes B: ***Automated searching for dactyloscopic data***

Annex B.1 Interface Control Document (ICD)

Annex B.2 Maximum Number of candidates accepted for verification

Annex B.3 Maximum research capacities per day for dactyloscopic data of identified persons

Annex B.4 Maximum research capacities per day for dactyloscopic fingerprinting traces

Annexes C: ***Automated searching for vehicle registration data***

Annex C.1 Common data-set for automated search of vehicle registration data

Annex C.2 Data Security

Annex C.3 Technical conditions of the data exchange

Annex C.4 List of contact points for incoming requests

Annexes D: ***Police cooperation***

Annex D.1 Procedures and contact points for the setting up of joint operations (article 24)

Annex D.2 Authorities to be notified without delay in case of a cross-border operation in the event of imminent danger and contact points for the reporting of modifications in the contact details listed in this Annex (article 25)

Annex D.3 Particular arms, ammunition and equipment which are prohibited to be carried according to article 28 paragraph 1, 3rd phrase of the Treaty, particular arms, ammunition and equipment which are prohibited to be used and the legal aspects according to article 28 paragraph 2 of the Treaty, practical aspects according to article 28 paragraph 5 of the Treaty

Annexes A

Automated searching for DNA profiles

Annex A.1

DNA related Forensic Issues, Matching Rules and Algorithms

Introduction

This document contains the requirements for DNA-profiles which are to be exchanged under the terms of the Treaty as well as the rules for matching and reporting. To enhance the exchangeability, existing (European and Interpol) standards are used.

Properties of DNA-profiles

The DNA profile contains 24 pairs of numbers representing the alleles of 24 loci which are also used in the DNA-procedures of Interpol. The names of these loci are shown in the following table:

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

The 7 grey loci in the top row are named the European Standard Set of Loci (ESS/ISSOL). The DNA-profiles made available by the Parties for searching and comparison as well as the DNA-profiles sent out for searching and comparison must contain at least 6 of 7 ESS/ISSOL loci and may contain the 17 other loci or blanks depending on their availability. In order to raise the accuracy of matches, it is recommended that all available alleles be stored in the indexed DNA profile data pool.

Mixed profiles or incomplete loci are not allowed so the allele values of each locus will consist of only 2 numbers, which may be the same in the case of homozygosity at a given locus.

Wild-cards and Micro-variants are to be dealt with upon the following rules:

- Any non-numerical value contained in the profile (e.g. “o”, “f”, “r”, “na”, “nr” or “un”) will be automatically converted to a wild-card and searched against all.
- Only numerical values “0”, “1” or “99” contained in the profile will be automatically converted to a wild-card and searched against all.

- If 3 alleles are provided for one locus the first allele will be accepted and the remaining 2 alleles converted to R (wild-card) and searched against all.
- When wild-card values are provided for allele 1 or 2 then both permutations of the numerical value given for the locus will be searched (e.g. 12,R could match against 12,14 or 9,12).
- Pentanucleotide (Penta D, Penta E & CD4) micro-variants will be matched according to the following:
  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
- Tetranucleotide (the rest of the Interpol database loci are tetranucleotides) micro-variants will be matched according to the following:
  x.1 = x, x.1, x.2
  x.2 = x.1, x.2, x.3
  x.3 = x.2, x.3, x+1

Matching rules

The comparison of 2 DNA-profiles will be performed on the basis of the loci for which a pair of allele values is available in both DNA-profiles. At least 6 loci of the ESS/ISSOL (exclusive of amelogenin) must be available in both DNA-profiles.

A full match is defined as a match, when all allele values of the compared loci commonly contained in the requesting and requested DNA-profiles are the same. A near match is defined as a match, when the value of only one of the all compared alleles is different in the 2 DNA profiles. A near match is only accepted if there are at least 6 fully matched loci in the 2 compared DNA profiles. The reason for a near match may be:

- A human typing error at the point of entry of one of the DNA-profiles in the search request or the DNA-database,
- an allele-determination or allele-calling error during the generation procedure of the DNA-profile.

Reporting rules

Both full matches and near matches will be reported.

The matching report will be sent to the requesting national contact point and will also be made available to the requested national contact point (to enable it to estimate the nature and number of possible follow-up requests for case and/or personal data associated with the DNA-profile corresponding to the hit).

Annex A.2

Party Code Number Table

Within the framework of the Treaty, it is decided to adopt ISO 3166-1 alpha-2 code for setting up the domain names and other configuration parameters required in the Prüm DNA data exchange applications over a closed network.

ISO 3166-1 alpha-2 codes are two-letter Party codes. They form the best known part of the standard ISO 3166-1 and (with a few changes) are used for Internet domain names.

Party Names	Code
Belgium	BE
Germany	DE
Spain	ES
France	FR
Luxembourg	LU
The Netherlands	NL
Austria	AT

Annex A.3

Functional Process and Workflow Analysis

1. WORKFLOW

This chapter contains the description of the workflow during the automated searching and comparison procedures of all the Parties databases (so called Prüm consultation), in compliance with the points 4.3 and 4.4 of the Implementing Agreement.

1.1 Data Transmission Procedure according to article 3 of the Treaty:

1.1.1 Unidentified DNA profile

- In case of a HIT in the national database on a reference DNA profile – no transmission.
- In case of a HIT in the national database with another unidentified DNA profile – no transmission. The comparison will be made in the framework of the procedure provided for in article 4 of the Treaty.
- In case of a NO-HIT in the national database – transmission to all databases if allowed by the Parties national legislation:
  - HIT on a reference DNA profile: automated notification of the HIT and transmission of profile(s) value(s).
  - HIT on an unidentified DNA profile: automated notification of the HIT and transmission of profile(s) value(s).
  - A note may be added in all national databases where a HIT was made – start of consultation process.
  - NO-HIT: automated NO-HIT notification.

1.1.2 Reference DNA profile

- In case of a HIT in the national database on a reference DNA profile – no transmission.
- In case of a HIT in the national database on an unidentified DNA profile – no transmission excepted if a note is added.
- In case of a HIT in the national database on a noted unidentified DNA profile – HIT abroad: second step of consultation process.
- In case of a NO-HIT in the national database – transmission to all databases if allowed by the Parties national legislation:
  - HIT on a reference DNA profile: automated notification of the HIT and transmission of profile(s) values.
  - HIT on an unidentified DNA profile: automated notification of the HIT and transmission of profile(s) value(s).
  - NO-HIT: automated NO-HIT notification.

1.2 Data Transmission Procedure according to article 4 of the Treaty:

As a first step, if allowed by the Parties national legislation, a search of all unidentified DNA profiles from crime scenes against the entire data stock of the Parties is made. Mass search for control purposes is possible later on.

- The initial comparison shall be made with unidentified DNA profiles.
- The following cases can occur:
  - In case of a HIT in the foreign databases on a reference DNA profile: automated notification of the HIT and transmission of profile(s) value(s) – second step of consultation process.
  - In case of HIT in the foreign databases on an unidentified DNA profile: automated notification of the HIT and transmission of profile(s) value(s) – second step of consultation process – it will be up to each Party to decide whether a note should be added in the databases. Following each Party's initiative, a special mention can be left in a database when a hit on an unidentified DNA profile occurred between a national DNA database and another Parties' DNA database.
  - In case of NO-HIT in the foreign databases: as the Treaty allows to regularly perform the comparisons, each Party will decide on the procedure (volume and frequency) to be undertaken for the comparison foreseen in article 4.
- If the national databases contain several identical profiles from different crimes, the requesting Party will transmit only one of these profiles for the matching process in order to avoid unnecessary duplication of work.
- Further details of this matching procedure referred to in article 4 of the Treaty shall be bilaterally agreed upon between the competent authorities.

2. FUNCTIONAL ANALYSIS: FIRST STEP

2.1 Declarations made in virtue of article 2 (3) of the Treaty:

AUSTRIA: Austria allows the national contact points of the other Parties access to the DNA reference data in its DNA analysis files, with the power to conduct automated searches by comparing DNA profiles, exclusively for the purpose of prosecuting criminal offences meeting the prerequisites for the issue of a European arrest warrant according to Article 2, paragraph 1 or 2, of the Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States, Official Journal No. L 190 of 18 July 2002, 1.

BELGIUM: Belgium will only make the DNA database of convicted offenders available to requesting Parties.

GERMANY: Pursuant to Article 2 (3) of the Treaty, Articles 2 to 6 thereof apply to the national DNA analysis file for the Federal Republic of Germany, which as a combined application is maintained at the Federal Criminal Police Office under Sections 2, 7 and 8 of the Federal Criminal Police Office Act and in the framework of the co-operation between the Federal Government and the Länder in criminal matters. The DNA analysis file is designed to attribute scene-of-crime marks to known criminal offenders with the aim of investigating criminal offences. For the purpose of data matching in the framework of the Treaty, solely reference data pursuant to Article 2 (2) sentence 2 of the Treaty is made available. Thus it is a subset of the data recorded in the DNA analysis file.

SPAIN: In accordance with article 2 (3) of the Treaty, articles 2 to 6 of the Treaty will apply to the file INT-SAIP, dependent of the Secretary of State of Security of the Ministry of the Interior of Spain. The purpose of this file is assistance to Justice Administration in investigations, by means of the genetic identification of biological traces and the identification of samples from known sources. This file stores information of criminal offences, identification and personal data. However, in accordance with article 2 (2) of the Treaty, only reference data from which the data subject cannot be directly identified will be made available to the Parties.

FRANCE: The consultation of the database is not allowed for minor offences (i.e., contravention).

NETHERLANDS: The Netherlands shall ensure the availability of reference data from its National DNA-analysis file for suspects, convicted offenders, deceased victims and biological stains from unsolved crimes.

LUXEMBOURG: For the purposes of automated DNA searching and comparison in compliance with the Treaty, Luxembourg grants the national contact points of the other Parties access to the DNA reference data of its two DNA databases as set up by the law of 25th August 2006 concerning DNA profiling in criminal matters: the DNA criminal database (including, *inter alia*, unidentified DNA profiles and the DNA profiles of suspected persons implied in an ongoing criminal investigation) and the DNA database of convicted offenders.

2.2 Volume/number of consultations

In order to implement efficiently the Treaty, each Party should be prepared to face the flow of requests which will occur.

Therefore, each Party made an estimation of the requests to which its own system will have to answer and an estimation of the consultations that it will make in the databases of the other Parties.

Estimated volume of consultations / year	**AT**	**BE**	**FR**	**DE**	**LU**	**NL**	**ES**
Unidentified DNA profiles	6 000	2 000	5 000	30 000	500	6 000	6 000
Reference DNA profiles	12 000	5 000	100 000	45 000	500	12 000	/

2.3 Availability of the system

The queries should reach the targeted database in the chronological order of arrival while the answer should reach the requesting Party within 15 minutes of the arrival of the query.

3. FUNCTIONAL ANALYSIS : SECOND STEP

When a Party receives a positive answer, the DNA expert undertakes a comparison between the values of the profile which was submitted in question and the values of the profile(s) which will be transmitted as an answer. The expert validates and checks the evidential value of the profile.

Legal assistance procedures start after a "full match" or a "near match" is obtained during the automated consultation phase and after validation of an existing match between two profiles.

Annex A.4

DNA Interface Control Document (ICD)

1. Introduction

1.1 Objectives

The purpose of this Annex is to define the requirements for the exchange of DNA profile information between the DNA database systems of all Parties. The header fields are defined specific for the Prüm DNA exchange, the data part is based on the DNA profile data part in the XML schema defined for the Interpol DNA exchange gateway.

It is agreed to exchange data by SMTP (Simple Mail Transfer Protocol), using a central relay mail server provided by the network provider. The XML file is transported as mail body.

1.2 Scope

This ICD defines the content of the message (mail) only. All network-specific and mail-specific topics are defined uniformly in order to allow a common technical base for the DNA data exchange.

Within this common definitions should be at least defined:
- The format of the subject field in the message to make an automated processing of the messages possible,
- if content encryption is necessary and if yes which methods should be chosen,
- the maximum length of messages.

1.3 XML structure and principles

The XML message is structured into
- header part, which contains information about the transmission and
- data part, which contains profile specific information + the profile itself.

The same XML schema should be useable for request and response. Fore purposes of complete checks of unidentified DNA profiles (Art. 4) it should be possible to send a batch of profiles in one message. A maximum number of profiles within one message must be defined. The number is depending from the maximum allowed mail size and should be defined after selection of the mail server.

XML example:

```
<?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>                datas structure repeated, if multiple profiles sent by
            (….)                a single SMTP message, only allowed for Art. 4 cases
        </datas>  ]
</PRUEMDNAx
```

2. XML Structure Definition

The following definitions are for documentation purposes and better readability, the real binding information is provided by an XML schema file (PRUEM DNA.xsd).

2.1 Schema PRUEMDNAx

It contains the following fields:

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

2.2 Content of Header structure

2.2.1 PRUEM_header

This is a structure describing the XML file header. It contains the following fields:

Fields	Type	Description
type	PRUEM_header_type	Type of the XML file
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 Party info
Requested	PRUEM_header_info	Requested Party info

2.2.2 PRUEM_header_type

Type of data contained in message, value can be:

Value	Description
M	Multiple Profiles (Art. 4)
S	Single Profile (Art. 3)

2.2.3 PRUEM_header_dir

Type of data contained in message, value can be:

Value	Description
R	Request
A	Answer

2.2.4 PRUEM_header_info

Structure to describe Party + message date/time. It contains the following fields:

Fields	**Type**	**Description**
Source_ISOCODE	string	ISO 3166-2 code of the Party
Destination_ISOCODE	String	
REQUEST_ID	String	unique Identifier for a request
date	date	Date of creation of message
time	Time	Time of creation of message

2.3 Content of PRUEM Profile datas

2.3.1 PRUEM_datas

This is a structure describing the XML profile data part. It contains the following fields:

Fields	**Type**	**Description**
date	Date	Date profile stored
type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of query
agency	String	Name of corresponding unit responsible for the profile
PROFILE_IDENT	String	Unique Party 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

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, in compliance with the points 4.3.7 and 4.4 of the Implementing Agreement.
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

2.3.2 PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

2.3.3 PRUEM_data_result

Type of data contained in message, value can be:

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

2.3.4 IPSG_DNA_profile

Structure describing a DNA profile. It contains the following fields:

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

2.3.5 IPSG_DNA_ISSOL

Structure containing the loci of ISSOL (Standard Group of Interpol loci). It contains the following fields:

Fields	Type	Description
Vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01
D21s11	IPSG_DNA_locus	Locus d21s11
Fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
Amelogenin	IPSG_DNA_locus	Locus amelogin

2.3.6 IPSG_DNA_additional_loci

Structure containing the other loci. It contains the following fields:

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

2.3.7 IPSG_DNA_locus

Structure describing a locus. It contains the following fields:

Fields	Type	Description
low_allele	String	Most low value of an allele
high_allele	String	Most high value of an allele

Annex A.5

Application, Security and Communication Architecture

1. Overview

In implementing applications for the DNA data exchange within the frame of the Treaty, it has been decided to use a common communication network, which will be logically closed among the Parties. In order to exploit this common communication infrastructure by sending requests and receiving replies in a more effective way, an asynchronous mechanism to convey DNA and dactyloscopic data requests in a wrapped SMTP e-mail message is adopted. In fulfillment of security concerns, the mechanism sMIME as extension to SMTP functionality will be used to establish a true end-to-end secure tunnel over the network.

The operative TESTA II (**T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations) has been chosen as the communication network for data exchange among the Parties. TESTA II is currently under the responsibility of the European Commission. In consideration of eventual different locations, where national DNA databases and the current national access points of TESTA II reside in the Parties sites, two options may be adopted to get the access to the TESTA II:

1) using the existing national access point or establishing a new national TESTA II access point, or
2) setting up a secure local link from the site, where DNA database resides and is administered by the corresponding national agency, to the existing national TESTA II access point.

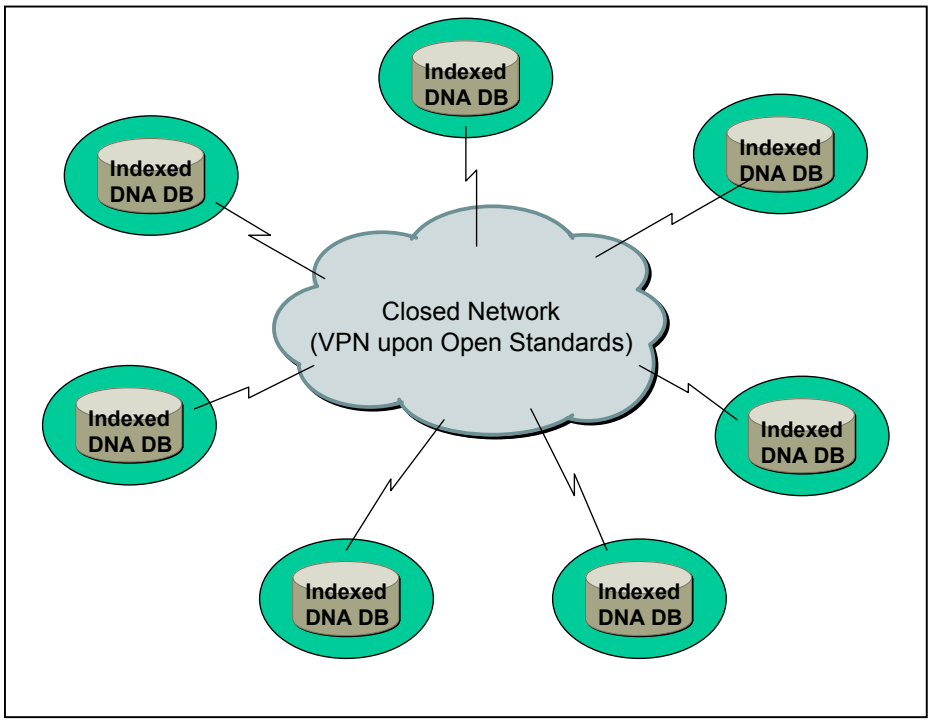
Each Party will decide which option to take by itself. This access scheme should be accepted by future acceding States to the Treaty.

The protocols and standards deployed in the implementation of the Treaty applications are in compliance with the Open Standards and meet the requirements imposed by national security policy makers of the Parties.

2. Upper Level Architecture

Each Party of the Treaty will make its DNA data available to be exchanged with and/or searched by other Parties in conformity with the standardized common data format. There exists no central computer server with a centralized database to hold DNA profiles.

Fig. 1: Topology of DNA Data Exchange



In addition to the fulfillment of national legal constraints at Parties' sites, each Party may decide by itself, what kind of hardware and software regarding the appropriate circumference should be deployed at its site to suit the needs of the Treaty.

3. Security Standards and Data Protection

Within the framework to implement the Treaty DNA data exchange, three levels of security concerns have concurred and will be deployed.

3.1 Data Level

DNA profile data provided by each Party has to be prepared in compliance with a common data protection standard, so that requesting Parties will receive an answer mainly to indicate HIT or NO-HIT along with an identification number in case of a HIT, which does not contain any personal information at all. The further investigation after the notification of a HIT will be conducted at the bilateral level upon the existing national legal and organizational regulations of the respective Parties' sites.

3.2 Communication Level

Messages containing DNA profile information (requesting and replying) will be encrypted upon a state-of-the-art mechanism corresponding to open standards before they are sent to other Parties' sites.

3.3 Transmission Level

All encrypted messages containing DNA profile information will be forwarded onto other Parties' sites through a virtual private tunneling system administered by a trust network provider at the international level and the secure links to this tunneling system under the national responsibility. This virtual private tunneling system does not have a connection point with the open Internet.

By exploiting advantages of these three security levels, DNA data exchange within the frame of the Treaty proves to satisfy a high security standard. By deployment of this three level security architecture the danger of the whole system being compromised to malicious attacks will be greatly mitigated.

4. Protocols and Standards to be used for encryption mechanism:

sMIME and related packages

In consideration of the technical requirements and available technologies, the open standard sMIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The current work on s/MIME (V3) is being done in the IETF's s/MIME Working Group. The protocol sMIME (V3) allows signed receipts, security labels, and secure mailing lists and layered on Cryptographic Message Syntax (CMS), an IETF specification for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data. The underlying certificate used by sMIME mechanism has to be in compliance with X.509 standard.

s/MIME functionality is built into the vast majority of modern e-mail software packages including Outlook, Mozilla Mail as well as Netscape Communicator 4.x and inter-operates among all major e-mail software packages.

Because of sMIME's easy integration into national IT infrastructure at all Parties' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal "Proof of Concept" in a more efficient way and reducing costs the open standard JavaMail API is however chosen for prototyping DNA data exchange. JavaMail API provides simple encryption and decryption of e-mails using s/MIME and/or OpenPGP. The intent is to provide a single, easy-to-use API for e-mail clients that want to send and received encrypted e-mail in either of the two most

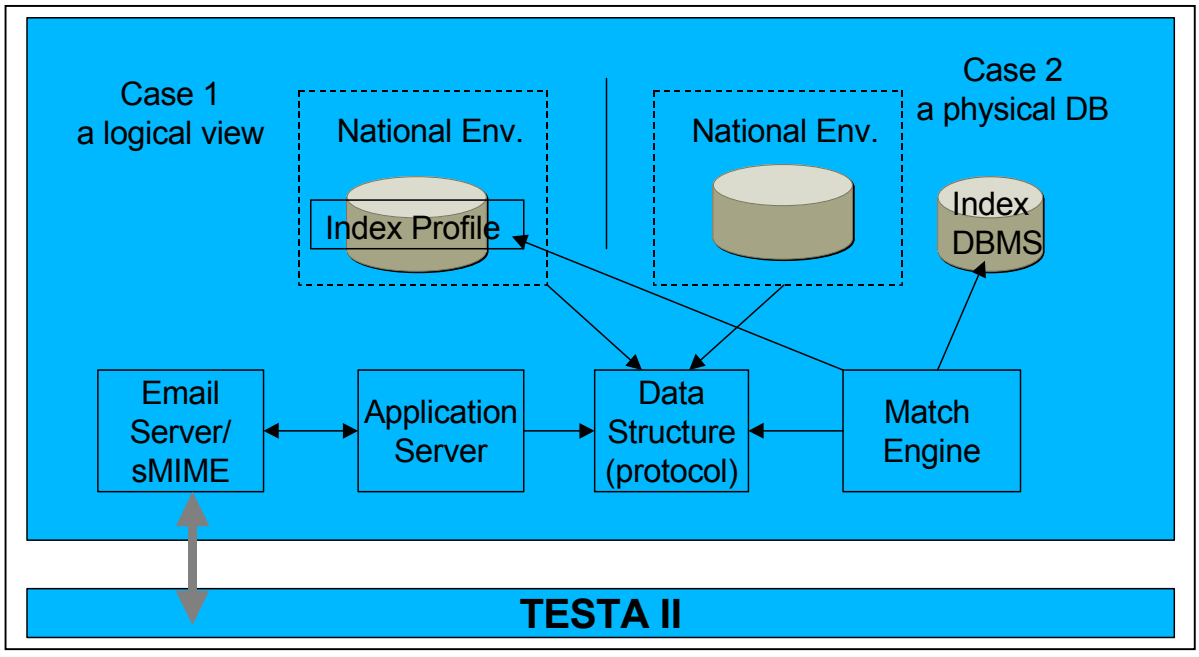
popular e-mail encryption formats. Therefore any state-of-the-art implementations to JavaMail API will suffice for the requirements set by the Treaty. For instance, the product of Bouncy Castle JCE (**J**ava **C**ryptographic **E**xtension) will be used to implement sMIME for prototyping DNA data exchange among all Parties.

5. Application Architecture

Each Party will provide the other Parties with a set of standardized DNA profile data upon the common ICD. There are two ways to make Treaty conformant DNA data available to the other Parties: construct a logical view over individual national database or establish a physical exported database. The four main components: E-mail server/sMIME, Application Server, Data Structure Area for fetching/feeding data and registering incoming/outgoing messages, and Match Engine implement the whole application logic in a product independent way. In order to provide all Parties with an easy integration of the components into their respective national sites, the same functionality will be implemented by optional open standards and protocols, which could be selected by each Party upon its national IT policy and regulations. Because of the neutral features to be implemented to get access to indexed databases containing Treaty conformant DNA profiles, each Party is given free choice to select its hardware and software platform including database and operating systems.

A prototype will be developed by a team consisting of the voluntary Parties with the goal to prove the concepts worked out. Other non-prototyping Parties could optionally adopt this prototype eventually with a certain amount of customization at local sites, but they are not obliged to take this product. Non-prototyping Parties may also develop their own products to get connected to the Treaty communication environment upon the specifications provided by the present Implementing Agreement.

Fig. 2: Overview Application Topology



6. Protocols and Standards to be used for application architecture:

6.1 XML

The DNA data exchange will fully exploit XML-schema as attachment to SMTP e-mail messages. The e**X**tensible **M**arkup **L**anguage (**XML**) is a W3C-recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data. The description of the DNA profile suitable for exchange among all Parties has been done by means of XML and XML schema in the ICD document.

6.2 ODBC

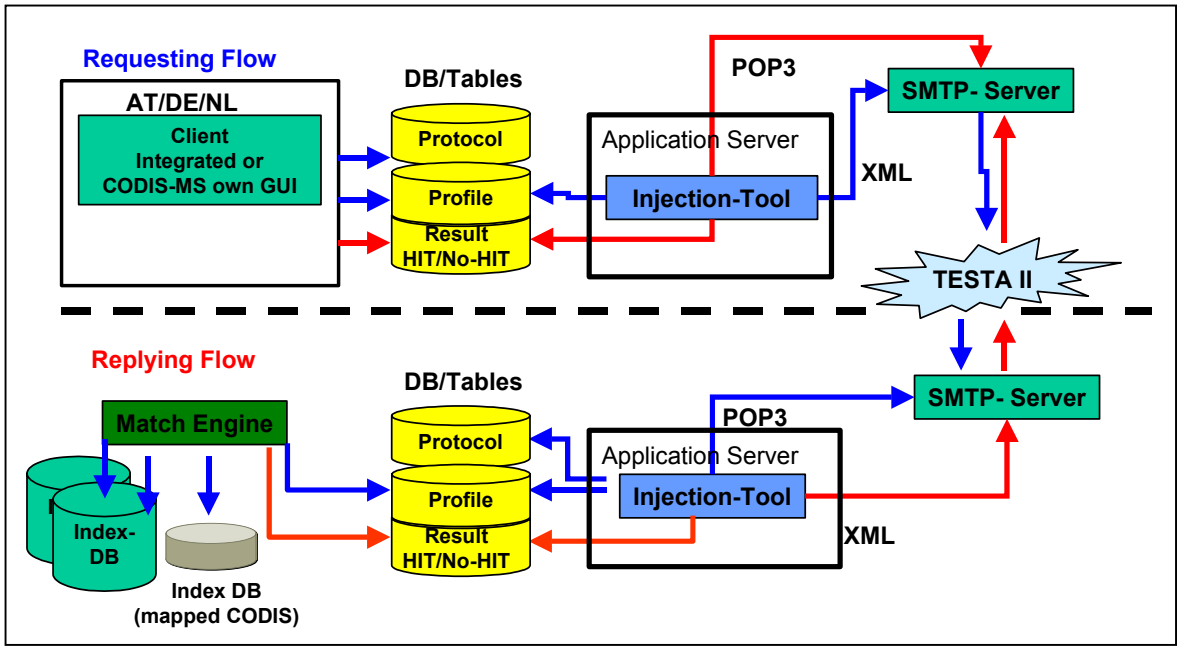
Open **D**ata**B**ase **C**onnectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has however certain drawbacks. Administering a large number of client machines can involve a diversity of drivers and DLLs. This complexity can increase system administration overhead.

6.3 JDBC

Java **D**ata**B**ase **C**onnectivity (**JDBC**) is an API for the Java programming language that defines how a client may access a database. In contrast to ODBC, JDBC does not require to use a certain set of local DLLs at the Desktop.

The business logic to process DNA profile requests and replies at each Parties' site is described in the following diagram. Both requesting and replying flows interact with a neutral data area comprising different data pools with a common data structure.

Fig. 3: Overview Application Architecture at each Parties' site



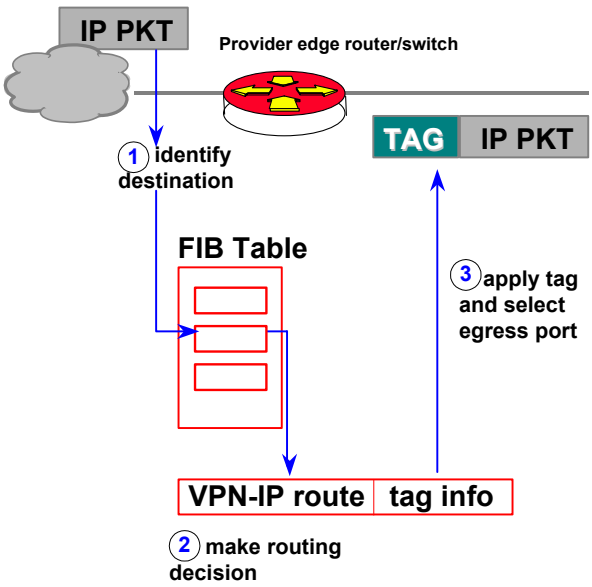
7. Communication Environment

7.1 Common Communication Network: TESTA II and its follow-up infrastructure

The application DNA data exchange will exploit the e-mail, an asynchronous mechanism, to send requests and to receive replies among the Parties. Upon the fact that all Parties do have at least one national access point to the TESTA II, the operation DNA data exchange will be deployed over the TESTA II network. TESTA II provides a number of added-value services through its e-mail relay. In addition to hosting TESTA II specific e-mail boxes, the infrastructure can implement mail distribution lists and routing policies. This allows TESTA II to be used as a clearing house for messages addressed to administrations connected to the Europe wide Domains. Virus check mechanisms can also be put in place. The TESTA II e-mail relay is built on a high availability hardware platform located at the central TESTA II application facilities and protected by firewall. The TESTA II **D**omain **N**ame **S**ervices (DNS) will resolve resource locators to IP addresses and hide addressing issues from the user and from applications.

7.2 Security Concern

The concept of a VPN (Virtual Private Network) has been implemented within the framework of TESTA II. Tag Switching Technology used to build this VPN will evolve to support Multi-Protocol Label Switching (MPLS) standard developed by the Internet Engineering Task Force (IETF).



MPLS is an IETF standard technology that speeds up network traffic flow by avoiding packet analysis by intermediate routers (hops). This is done on the basis of so-called labels that are attached to packet by the edge routers of the backbone, on the basis of information stored in the forwarding information base (FIB). Labels are also used to implement virtual private networks (VPNs).

MPLS combines the benefits of layer 3 routing with the advantages of layer 2 switching. Because IP addresses are not evaluated during transition through the backbone, MPLS does not impose any IP addressing limitations.

Furthermore e-mail messages over the TESTA II will be protected by sMIME driven encryption mechanism. Without knowing the key and possessing the right certificate, nobody can decrypt messages over the network.

7.3 Protocols and Standards to be used over the communication network

7.3.1 SMTP

Simple **M**ail **T**ransfer **P**rotocol is the *de facto* standard for e-mail transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and then the message text is transferred. SMTP uses TCP port 25 upon the specification by the IETF. To determine the SMTP server for a given domain name, the MX (Mail eXchange) DNS (Domain Name Systems) record is used.

Since this protocol started as purely ASCII text-based it did not deal well with binary files. Standards such as MIME were developed to encode binary files for transfer through SMTP. Today, most SMTP servers support the 8BITMIME and sMIME extension, permitting binary files to be transmitted almost as easily as plain text.

SMTP is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Within the framework of implementing DNA data exchange it is decided to use the protocol POP3.

7.3.2 POP

Local e-mail clients use the **P**ost **O**ffice **P**rotocol version **3** (**POP3**), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection. By using the SMTP Submit profile of the SMTP protocol, e-mail clients send messages across the Internet or over a corporate network. MIME serves as the standard for attachments and non-ASCII text in e-mail. Although neither POP3 nor SMTP requires MIME-formatted e-mail, essentially Internet e-mail comes MIME-formatted, so POP clients must also understand and use MIME. The whole communication environment of the Treaty will therefore include the components of POP.

7.4 Network Address Scheme

The address block 62.62.0.0/17 has currently been allocated by the European IP registration authority (RIPE) to TESTA II. Further address blocks may be allocated to TESTA II in the future if required (but for that, at least 80% of the 62.62.0.0/17 should be already assigned, and actually used in the TESTA II network). The address space allocated to the TESTA II network is 62.62.0.0 – 62.62.127.255. Considering the geographical approach as introduced above, for each country a dedicated block of C class sub-nets is allocated.

For the current Parties, the IP address ranges are assigned to and/or reserved for by the administration of TESTA II in the following table:

IP address range	Parties	comments
62.62.0.0/24 – 62.62.1.0/24	Central Service (TESTA II)	
62.62.30.0/24 – 62.62.33.0/24	Austria	
62.62.22.0/24 – 62.62.25.0/24	Belgium	
62.62.50.0/24	France	
62.62.38.0/24 to 62.62.40.0/24	Germany	first part

IP address range	Parties	comments
62.62.76.0/24 to 62.62.79.0/24	Germany	second part
62.62.54.0/24	The Netherlands	
62.62.26.0/24 – 62.62.29.0/24	Luxemburg	
62.62.6.0/24 – 62.62.9.0/24	Spain	

The IP address ranges are subject to change during the further development of TESTA II.

7.5 Configuration Parameters

A secure e-mail system is set up using the **eu-admin.net** domain. This domain with the associated addresses will not be accessible from a location not on the TESTA II Europe wide domain, because the names are only known on the TESTA II central DNS server, which is shielded from the Internet.

The resolution of these TESTA II site addresses (host names) to their IP addresses is done by the TESTA II DNS service. For each Local Domain, a Mail entry will be added to this TESTA II central DNS server, making all e-mail messages sent to TESTA Local Domains being relayed to the TESTA II central Mail Relay. This TESTA II central Mail Relay will then forward them to the specific Local Domain e-mail server using the Local Domain e-mail addresses. By relaying the e-mail in this way, critical information contained in e-mails will only pass the Europe wide closed network infrastructure and not the insecure Internet.

It is necessary to establish sub domains (***bold italics***) in all Parties' sites upon the following syntax:
"***application-type*.pruem.*party-code*.**eu-admin.net", where:
"party-code" takes one of the values: AT, BE, DE, ES, FR, LU and NL; the party code is a country code;
"***application-type***" takes one of the values: DNA and FP.

By applying the above syntax, the sub domains for the current seven Parties are shown in the following table:

MS/Parties	Sub Domains	Comments
Austria	***dna*.pruem.at**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.at**.eu-admin.net	
Belgium	***dna*.pruem.be**.eu-admin.net	Setting up a secure local link to the existing TESTA II access point
	***fp*.pruem.be**.eu-admin.net	
Germany	***dna*.pruem.de**.eu-admin.net	Using the existing TESTA II national access points
	***fp*.pruem.de**.eu-admin.net	
Spain	***dna*.pruem.es**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.es**.eu-admin.net	
France	***dna*.pruem.fr**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.fr**.eu-admin.net	
Luxemburg	***dna*.pruem.lu**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.lu**.eu-admin.net	

MS/Parties	Sub Domains	Comments
The Netherlands	***dna*.pruem.nl**.eu-admin.net	Intending to establish a new TESTA II access point at the NFI
	***fp*.pruem.nl**.eu-admin.net	

8. Conclusion

Upon the result of negotiations with the European Commission (EU COM), a step-by-step approach to deploy the DNA application over TESTA II will be adopted. A certain amount of customization work has to be done mainly by the EU COM in joint work with the TESTA II provider. However, each Party is in charge of the necessary modifications for the IT environment at its respective sites if requested. The first deployment step over TESTA II is planned among the prototyping Parties and the other Parties may have the deployment at a ready-to-go basis after the fulfilment of the necessary requirements from IT and organizational point of view. A requirement sheet to be filled out by non-prototyping Parties will be sent out timely before the deployment commences.

Annexes B

Automated searching for dactyloscopic data

Annex B.1

Interface Control Document (Dactyloscopic data)

Introduction

The purpose of this document is to define the requirements for the exchange of dactyloscopic information between the Automated Fingerprint Identification Systems (AFIS) of the Parties. It is based on the Interpol-Implementation of ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b).

This version shall cover all basic definitions for Logical Records Type-1, Type-2, Type-4, Type-9, Type-13 and Type-15 required for image and minutiæ based dactyloscopic processing.

1. File Content Overview

A dactyloscopic file consists of several logical records. There are sixteen types of record specified in the original ANSI/NIST-ITL 1-2000 standard. Appropriate ASCII separation characters are used between each record and the fields and subfields within the records.

In this version for the application of the Treaty, only 6 record types are used to exchange information between the originating and the destination agency:

Type-1 -> Transaction information
Type-2 -> Alphanumeric persons/case data
Type-4 -> High resolution grayscale dactyloscopic images
Type-9 -> Minutiæ Record
Type-13 -> Variable resolution latent image
Type-15 -> Variable resolution palmprint image record

1.1 Type-1 – File header

This record contains routing information and information describing the structure of the rest of the file. This record type also defines the types of transaction which fall under the following broad categories:

1.2 Type-2 – Descriptive text

This record contains textual information of interest to the sending and receiving agencies.

1.3 Type-4 – High resolution gray-scale image

This record is used to exchange high resolution gray-scale (eight bit) dactyloscopic images sampled at 500 pixels/inch. The dactyloscopic images shall be compressed using the WSQ algorithm with a ratio not more than 15:1. Other compression algorithms or uncompressed images must not be used.

1.4 Type-9 – Minutiæ record

Type-9 records are used to exchange ridge characteristics or minutiæ data. Their purpose is partly to avoid unnecessary duplication of AFIS encoding processes and partly to allow the transmission of AFIS codes which contain less data than the corresponding images.

1.5 Type-13 – Variable-Resolution Latent Image Record

This record shall be used to exchange variable-resolution latent fingerprint and latent palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 gray-levels. If the quality of the latent image is sufficient it shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 gray-levels on bilateral agreement.

1.6 Variable-Resolution Palmprint Image Record

Type-15 tagged field image records shall be used to exchange variable-resolution palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 gray-levels. To minimize the amount of data all palmprint images shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 gray-levels on bilateral agreement.

2. Record format

A transaction file shall consist of one or more logical records. For each logical record contained in the file, several information fields appropriate to that record type shall be present. Each information field may contain one or more basic single-valued information items. Taken together these items are used to convey different aspects of the data contained in that field. An information field may also consist of one or more information items grouped together and repeated multiple times within a field. Such a group of information items is known as a subfield. An information field may therefore consist of one or more subfields of information items.

2.1 Information separators

In the tagged-field logical records, mechanisms for delimiting information are implemented by use of four ASCII information separators. The delimited information may be items within a field or subfield, fields within a logical record, or multiple occurrences of subfields. These information separators are defined in the standard ANSI X3.4. These characters are used to separate and qualify information in a logical sense. Viewed in a hierarchical relationship, the File Separator "FS" character is the most inclusive followed by the Group Separator "GS", the Record Separator "RS", and finally the Unit Separator "US" characters. Table 1 lists these ASCII separators and a description of their use within this standard.

Information separators should be functionally viewed as an indication of the type data that follows. The "US" character shall separate individual information items within a field or subfield. This is a signal that the next information item is a piece of data for that field or subfield. Multiple subfields within a field separated by the "RS" character signals the start of the next group of repeated information item(s). The "GS" separator character used between information fields signals the beginning of a new field preceding the field identifying number that shall appear. Similarly, the beginning of a new logical record shall be signalled by the appearance of the "FS" character.

The four characters are only meaningful when used as separators of data items in the fields of the ASCII text records. There is no specific meaning attached to these characters occurring in binary image records and binary fields – they are just part of the exchanged data.

Normally, there should be no empty fields or information items and therefore only one separator character should appear between any two data items. The exception to this rule occurs for those instances where the data in fields or information items in a transaction are unavailable, missing, or optional, and the processing of the transaction is not dependent upon the presence of that particular data. In those instances, multiple and adjacent separator characters shall appear together rather than requiring the insertion of dummy data between separator characters.

Consider the definition of a field that consists of three information items. If the information for the second information item is missing, then two adjacent "US" information separator characters would occur between the first and third information items. If the second and third information items were both missing, then three separator characters should be used – two "US" characters in addition to the terminating field or subfield separator character. In general, if one or more mandatory or optional information items are unavailable for a field or subfield, then the appropriate number of separator character should be inserted.

It is possible to have side-by-side combinations of two or more of the four available separator characters. When data are missing or unavailable for information items, subfields, or fields, there must be one fewer separator characters present than the number of data items, subfields, or fields required.

Table 1: Separators Used

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 Record layout

For tagged-field logical records, each information field that is used shall be numbered in accordance with this standard. The format for each field shall consist of the logical record type number followed by a period ".", a field number followed by a colon ":", followed by the information appropriate to that field. The tagged-field number can be any one-to nine-digit number occurring between the period "." and the colon ":". It shall be interpreted as an unsigned integer field number. This implies that a field number of "2.123:" is equivalent to and shall be interpreted in the same manner as a field number of "2.000000123:".

For purposes of illustration throughout this document, a three-digit number shall be used for enumerating the fields contained in each of the tagged-field logical records described herein. Field numbers will have the form of "TT.xxx:" where the "TT" represents the one- or two-character record type followed by a period. The next three characters comprise the appropriate field number followed by a colon. Descriptive ASCII information or the image data follows the colon.

Logical Type-1 and Type-2 records contain only ASCII textual data fields. The entire length of the record (including field numbers, colons, and separator characters) shall be recorded as the first ASCII field within each of these record types. The ASCII File Separator "FS" control character (signifying the end of the logical record or transaction) shall follow the last byte of ASCII information and shall be included in the length of the record.

In contrast to the tagged-field concept, the Type-4 record contains only binary data recorded as ordered fixed-length binary fields. The entire length of the record shall be recorded in the first four-byte binary field of each record. For this binary record, neither the record number with its period, nor the field identifier number and its following colon, shall be recorded. Furthermore, as all the field lengths of this record is either fixed or specified, none of the four separator characters ("US", "RS", "GS", or "FS") shall be interpreted as anything other than binary data. For the binary record, the "FS" character shall not be used as a record separator or transaction terminating character.

3. Type-1 Logical Record: the File Header

This record describes the structure of the file, the type of the file, and other important information. The character set used for Type-1 fields shall contain only the 7-bit ANSI code for information interchange.

3.1 Fields for Type-1 Logical Record

3.1.1 Field 1.001: Logical Record Length (LEN)

This field contains the total count of the number of bytes in the whole Type-1 logical record. The field begins with “1.001:”, followed by the total length of the record including every character of every field and the information separators.

3.1.2 Field 1.002: Version Number (VER)

To ensure that users know which version of the ANSI/NIST standard is being used, this four byte field specifies the version number of the standard being implemented by the software or system creating the file. The first two bytes specify the major version reference number, the second two the minor revision number. For example, the original 1986 Standard would be considered the first version and designated “0100” while the present ANSI/NIST-ITL 1-2000 standard is “0300”.

3.1.3 Field 1.003: File Content (CNT)

This field lists each of the records in the file by record type and the order in which the records appear in the logical file. It consists of one or more subfields, each of which in turn contains two information items describing a single logical record found in the current file. The subfields are entered in the same order in which the records are recorded and transmitted.

The first information item in the first subfield is "1", to refer to this Type-1 record. It is followed by a second information item which contains the number of other records contained in the file. This number is also equal to the count of the remaining subfields of field 1.003.

Each of the remaining subfields is associated with one record within the file, and the sequence of subfields corresponds to the sequence of records. Each subfield contains two items of information. The first is to identify the Type of the record. The second is the record's IDC. The "*US*" character shall be used to separate the two information items.

3.1.4 Field 1.004: Type of Transaction (TOT)

This field contains a three letter mnemonic designating the type of the transaction. These codes may be different from those used by other implementations of the ANSI/NIST standard.

CPS: Criminal Print-to-Print Search. This transaction is a request for a search of a record relating to a criminal offence against a prints database. The person’s prints must be included as WSQ-compressed images in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record
⇒ 1-14 Type-4 Record

The CPS TOT is summarized in **Table A.6.1** (Appendix 6).

PMS: Print-to-Latent Search. This transaction is used when a set of prints shall to be searched against an Unidentified Latent database. The response will contain the **Hit/No-Hit** decision of the destination AFIS search. If multiple unidentified latents exist, multiple SRE transactions will be returned, with one latent per transaction. The person's prints must be included as WSQ-compressed images in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record
⇒ 1 Type-13 Record

The PMS TOT is summarized in **Table A.6.1 (**Appendix 6**).**

MPS: Latent-to-Print Search. This transaction is used when a latent is to be searched against a Prints database. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record
⇒ 1 Type-4 or Type-15 Record

The MPS TOT is summarized in **Table A.6.4 (**Appendix 6**)**.

MMS: Latent-to-Latent Search. In this transaction the file contains a latent which is to be searched against an Unidentified Latent database in order to establish links between various scenes of crime. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record
⇒ 1 Type-13 Record

The MMS TOT is summarized in **Table A.6.4 (**Appendix 6**)**.

SRE: This transaction is returned by the destination agency in response to dactyloscopic submissions. The response will contain the **Hit/No-Hit** decision of the destination AFIS search. If multiple candidates exist, multiple SRE transactions will be returned, with one candidate per transaction.
The SRE TOT is summarized in **Table A.6.2 (**Appendix 6**)**.

ERR: This transaction is returned by the destination AFIS to indicate a transaction error. It includes a message field (**ERM**) indicating the error detected. The following logical records will be returned:

⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

The ERR TOT is summarized in **Table A.6.3** (Appendix 6).

Table 2: Permissible Codes in Transactions

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	-
MMS	M	M	-	M (1*)	M	-
PMS	M	M	M*	-	-	M*
ERR	M	M	-	-	-	-

Key:
M = Mandatory
M* = Only one of both record-types may be included
O = Optional
C = Conditional if data is available
- = Not allowed
1* = Conditional for legacy systems

3.1.5 Field 1.005: Date of Transaction (DAT)

This field indicates the date on which the transaction was initiated and must conform to the ISO standard notation of: YYYYMMDD
where YYYY is the year, MM is the month and DD is the day of the month. Leading zeros are used for single figure numbers. For example, "19931004" represents the 4 October 1993.

3.1.6 Field 1.006: Priority (PRY)

This optional field defines the priority, on a level of 1 to 9, of the request. "1" is the highest priority and "9" the lowest. Accordingly to the Implementing Agreement, priority "1" transactions shall be processed immediately.

3.1.7 Field 1.007: Destination Agency Identifier (DAI)

This field specifies the destination agency for the transaction.
It consists of two information items in the following format: CC/*agency*.
The first information item contains the Country Code, defined in ISO 3166, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

3.1.8 Field 1.008: Originating Agency Identifier (ORI)

This field specifies the file originator and has the same format as the DAI (Field 1.007).

3.1.9 Field 1.009: Transaction Control Number (TCN)

This is a control number for reference purposes. It should be generated by the computer and have the following format: YYSSSSSSSSA
where YY is the year of the transaction, SSSSSSSS is an eight-digit serial number, and A is a check character generated by following the procedure given in Appendix 2.
Where a TCN is not available, the field, YYSSSSSSSS, is filled with zeros and the check character generated as above.

3.1.10 Field 1.010: Transaction Control Response (TCR)

Where a request was sent out, to which this is the response, this optional field will contain the transaction control number of the request message. It therefore has the same format as TCN (Field 1.009).

3.1.11 Field 1.011: Native Scanning Resolution (NSR)

This field specifies the normal scanning resolution of the system supported by the originator of the transaction. The resolution is specified as two numeric digits followed by the decimal point and then two more digits.
For all transactions linked to the Treaty the sampling rate shall be 500 pixels/inch or 19.68 pixels/mm.

3.1.12 Field 1.012: Nominal Transmitting Resolution (NTR)

This five-byte field specifies the nominal transmitting resolution for the images being transmitted. The resolution is expressed in pixels/mm in the same format as NSR (Field 1.011).

3.1.13 Field 1.013: Domain name (DOM)

This mandatory field identifies the domain name for the user-defined Type-2 logical record implementation. It consists of two information items and shall be “INT-I{US}4.22{GS}”.

3.1.14 Field 1.014: Greenwich meantime (GMT)

This mandatory field provides a mechanism for expressing the date and time in terms of universal Greenwich Mean Time (GMT) units. If used, the GMT field contains the universal date that will be in addition to the local date contained in Field 1.005 (DAT). Use of the GMT field eliminates local time inconsistencies encountered when a transaction and its response are transmitted between two places separated by several time zones. The GMT provides a universal date and 24-hour clock time independent of time zones. It is represented as "CCYYMMDDHHMMSSZ”, a 15-character string that is the concatenation of the date with the GMT and concludes with a “Z”. The “CCYY” characters shall represent the year of the transaction, the “MM” characters shall be the tens and units values of the month, and the “DD” characters shall be the tens and units values of the day of the month, the “HH” characters rep-resent the hour, the “MM” the minute, and the “SS” represents the second. The complete date shall not exceed the current date.

4. Type-2 Logical Record: Descriptive Text

The structure of most of this record is not defined by the original ANSI/NIST standard. The record contains information of specific interest to the agencies sending or receiving the file. To ensure that communicating dactyloscopic systems are compatible this ICD requires that only the fields listed below are contained within the record. This document specifies which fields are mandatory and which optional, and also defines the structure of the individual fields.

4.1 Fields for Type-2 Logical Record

4.1.1 Field 2.001: Logical Record Length (LEN)

This mandatory field contains the length of this Type-2 record, and specifies the total number of bytes including every character of every field contained in the record and the information separators.

4.1.2 Field 2.002: Image Designation Character (IDC)

The IDC contained in this mandatory field is an ASCII representation of the IDC as defined in the file content field of the Type-1 record.

4.1.3 Field 2.003: System Information (SYS)

This field is mandatory and contains four bytes which indicate which version of the INT-I this particular Type-2 record complies with.

The first two bytes specify the major version number, the second two the minor revision number. For example, this implementation is based on INT-I version 4 revision 22 and would be represented as "0422".

4.1.4 Field 2.007: Case Number (CNO)

This is a number assigned by the local dactyloscopic bureau to a collection of latents found at a scene-of-crime. The following format is adopted: CC/*number*
where CC is the Interpol Country Code, two alpha-numeric characters in length, and the *number* complies with the appropriate local guidelines and may be up to 32 alpha-numeric characters long.

This field allows the system to identify latents associated with a particular crime.

4.1.5 Field 2.008: Sequence Number (SQN)

This specifies each sequence of latents within a case. It can be up to four numeric characters long. A sequence is a latent or series of latents which are grouped together for the purposes of filing and/or searching. This definition implies that even single latents will still have to be assigned a sequence number.

This field together with MID (Field 2.009) may be included to identify a particular latent within a sequence.

4.1.6 Field 2.009: Latent Identifier (MID)

This specifies the individual latent within a sequence. The value is a single letter, with 'A' assigned to the first latent, 'B' to the second, and so on up to a limit of 'J'. This field is used analog to the latent sequence number discussed in the description for SQN (Field 2.008).

4.1.7 Field 2.010: Criminal Reference Number (CRN)

This is a unique reference number assigned by a national agency to an individual who is charged for the first time with committing an offence. Within one country no individual ever has more than one CRN, or shares it with any other individual. However, the same individual may have Criminal Reference Numbers in several countries, which will be distinguishable by means of the country code.

The following format is adopted for CRN field: CC/*number*
where CC is the Country Code, defined in ISO 3166, two alpha-numeric characters in length, and the *number* complies with the appropriate national guidelines of the issuing agency, and may be up to 32 alpha-numeric characters long.

For transactions linked to the Treaty this field will be used for the national criminal reference number of the originating agency which is linked to the images in Type-4 or Type-15 Records.

4.1.8 Field 2.012: Miscellaneous Identification Number (MN1)

This fields contains the CRN (field 2.010) transmitted by an CPS or PMS transaction without the leading country code.

4.1.9 Field 2.013: Miscellaneous Identification Number (MN2)

This fields contains the CNO (field 2.007) transmitted by an MPS or MMS transaction without the leading country code.

4.1.10 Field 2.014: Miscellaneous Identification Number (MN3)

This fields contains the SQN (field 2.008) transmitted by an MPS or MMS transaction.

4.1.11 Field 2.015: Miscellaneous Identification Number (MN4)

This fields contains the MID (field 2.009) transmitted by an MPS or MMS.

4.1.12 Field 2.063: Additional Information (INF)

This optional field, consisting of up to 32 alpha-numeric characters, may give additional information about the request.

4.1.13 Field 2.064: Respondents List (RLS)

This field contains at least two subfields. The first subfield describes the type of search that has been carried out, using the three-letter mnemonics which specify the transaction type in TOT (Field 1.004). The second subfield contains a single character. An "**I**" shall be used to indicate that a HIT has been found and an "**N**" shall be used to indicate that no matching cases have been found (NOHIT). The third subfield contains the sequence identifier for the candidate result and the total number of candidates separated by a slash. Multiple messages will be returned if multiple candidates exist.

In case of a possible HIT the fourth subfield shall contain the score up to six digits long. If the HIT has been verified the value of this subfield is defined as "999999".

Example: "CPS{RS}I{RS}001/001{RS}999999{GS}"

If the remote AFIS does not assign scores, then a score of zero should be used at the appropriate point.

4.1.14 Field 2.074: Status/Error Message Field (ERM)

This field contains error messages resulting from transactions, which will be sent back to the requester as part of an Error Transaction.

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.

Error messages in the range between 100 and 199:

These error messages are related to the validation of the ANSI/NIST records and defined as:
<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>…
where

- error_code is a code uniquely related to a specific reason (see table)
- field_id is the ANSI/NIST field number of the incorrect field (e.g. 1.001, 2.001, ...) in the format <record_type>.<field_id>.<sub_field_id>
- dynamic text is a more detailed dynamic description of the error
- LF is a Line Feed separating errors if more then one error is encountered
- for type-1 record the ICD is defined as "-1"

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

This field is mandatory for error transactions.

4.1.15 Field 2.320: Expected Number of Candidates (ENC)

This field contains the maximum number of candidates for verification expected by the requesting agency. The value of ENC must not exceed the values defined in Annex B.2 of this Implementing Agreement.

5. Type-4 Logical Record: High Resolution Gray-Scale Image

It should be noted that Type-4 records are binary rather than ASCII in nature. Therefore each field is assigned a specific position within the record, which implies that all fields are mandatory.

The standard allows both image size and resolution to be specified within the record. It requires Type-4 Logical Records to contain dactyloscopic image data that are being transmitted at a nominal pixel density of 500 to 520 pixels per inch. The preferred rate for new designs is at a pixel density of 500 pixels per inch or 19.68 pixels per mm. 500 pixels per inch is the density specified by the INT-I, except that similar systems may communicate with each other at a non-preferred rate, within the limits of 500 to 520 pixels per inch.

5.1 Fields for Type-4 Logical Record

5.1.1 Field 4.001: Logical Record Length (LEN)

This four-byte field contains the length of this Type-4 record, and specifies the total number of bytes including every byte of every field contained in the record.

5.1.2 Field 4.002: Image Designation Character (IDC)

This is the one-byte binary representation of the IDC number given in the header file.

5.1.3 Field 4.003: Impression Type (IMP)

The impression type is a single-byte field occupying the sixth byte of the record.

Table 3 : Finger Impression Type

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

Code	Description
4	Latent impression captured directly
5	Latent tracing
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4 Field 4.004: Finger Position (FGP)

This fixed-length field of 6 bytes occupies the seventh through twelfth byte positions of a Type-4 record. It contains possible finger positions beginning in the left most byte (byte 7 of the record). The known or most probable finger position is taken from the following table. Up to five additional fingers may be referenced by entering the alternate finger positions in the remaining five bytes using the same format. If fewer than five finger position references are to be used the unused bytes are filled with binary 255. To reference all finger positions code 0, for unknown, is used.

Table 4: Finger position code and maximum size

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

For scene of crime latents only the codes 0 to 10 should be used.

5.1.5 Field 4.005: Image Scanning Resolution (ISR)

This one-byte field occupies the 13th byte of a Type-4 record. If it contains “0” then the image has been sampled at the preferred scanning rate of 19.68 pixels/mm (500 pixels per inch). If it contains “1” then the image has been sampled at an alternative scanning rate as specified in the Type-1 record.

5.1.6 Field 4.006: Horizontal Line Length (HLL)

This field is positioned at bytes 14 and 15 within the Type-4 record. It specifies the number of pixels contained in each scan line. The first byte will be the most significant.

5.1.7 Field 4.007: Vertical Line Length (VLL)

This field records in bytes 16 and 17 the number of scan lines present in the image. The first byte is the most significant.

5.1.8 Field 4.008: Gray-scale Compression Algorithm (GCA)

This one-byte field specifies the gray-scale compression algorithm used to encode the image data. A binary zero indicates that no compression algorithm has been used. In this case pixels are recorded in left to right, top to bottom fashion. The FBI will maintain a registry relating non-zero numbers to compression algorithms. This Implementation based on the INT-I will use the same allocation of numbers.

5.1.9 Field 4.009: The Image

This field contains a byte stream representing the image. Its structure will obviously depend on the compression algorithm used.

6. Type-9 Logical Record: Minutiæ Record

Type-9 records shall contain ASCII text describing minutiæ and related information encoded from a latent. For latent search transaction, there no limit for these Type-9 records in a file, each of which shall be for a different view or latent.

6.1 Minutiæ extraction

6.1.1 Minutia type identification

This standard defines three identifier numbers that are used to describe the minutia type. These are listed in Table 4.1. A ridge ending shall be designated Type 1. A bifurcation shall be designated Type 2. If a minutia cannot be clearly categorized as one of the above two types, it shall be designated as “other”, Type 0.

Table 5: Minutia types

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2 Minutia placement and type

For templates to be compliant with Section 5 of the ANSI INCITS 378-2004 standard, the following method, which enhances the current INCITS 378-2004 standard, shall be used for determining placement (location and angular direction) of individual minutiae.

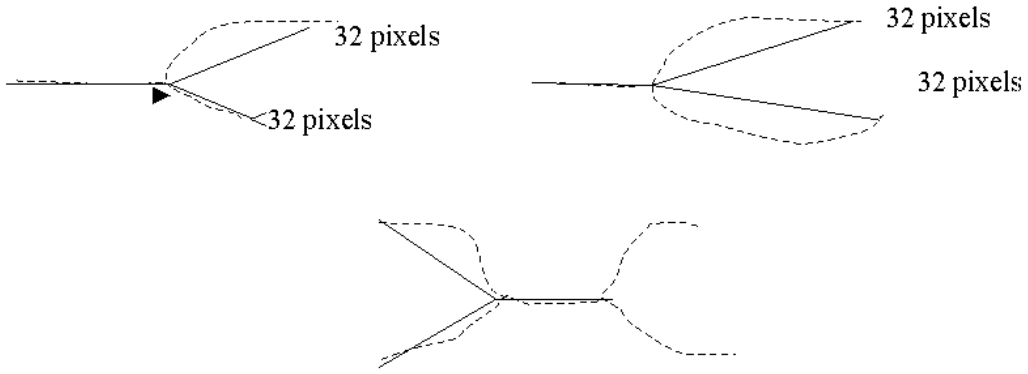
The position or location of a minutia representing a ridge ending shall be the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the three legs of the valley area were thinned down to a single-pixel-wide skeleton, the point of the intersection is the location of the minutia. Similarly, the location of the minutia for a bifurcation shall be the point of forking of the medial skeleton of the ridge. If the three legs of the ridge were each thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia.

After all ridge endings have been converted to bifurcations, all of the minutiae of the dactyloscopic image are represented as bifurcations. The X and Y pixel coordinates of the intersection of the three legs of each minutia can be directly formatted. Determination of the minutia direction can be extracted from each skeleton bifurcation. The three legs of every skeleton bifurcation must be examined and the endpoint of each leg determined. Figure 6.1.2 illustrates the three methods used for determining the end of a leg that is based on a scanning resolution of 500 ppi.

The ending is established according to the event that occurs first. The pixel count is based on a scan resolution of 500 ppi. Different scan resolutions would imply different pixel counts.

- A distance of .064" (the 32nd pixel)
- The end of skeleton leg that occurs between a distance of .02" and .064" (the 10th through the 32nd pixels); shorter legs are not used
- A second bifurcation is encountered within a distance of .064" (before the 32nd pixel)

Figure 6.1.2



The angle of the minutiae is determined by constructing three virtual rays originating at the bifurcation point and extending to the end of each leg. The smallest of the three angles formed by the rays is bisected to indicate the minutiae direction.

6.1.3 Coordinate system

The coordinate system used to express the minutiae of a fingerprint shall be a Cartesian coordinate system. Minutiae locations shall be represented by their x and y coordinates. The origin of the coordinate system shall be the upper left corner of the original image with x increasing to the right and y increasing downward. Both x and y coordinates of a minutiae shall be represented in pixel units from the origin. It should be noted that the location of the origin and units of measure is not in agreement with the convention used in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.1.4 Minutiæ direction

Angles are expressed in standard mathematical format, with zero degrees to the right and angles increasing in the counter clockwise direction. Recorded angles are in the direction pointing back along the ridge for a ridge ending and toward the centre of the valley for a bifurcation. This convention is 180 degrees opposite of the angle convention described in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.2 Fields for Type-9 Logical record INCITS-378 Format

All fields of the Type-9 records shall be recorded as ASCII text. No binary fields are permissible in this tagged-field record.

6.2.1 Field 9.001: Logical record length (LEN)

This mandatory ASCII field shall contain the length of the logical record specifying the total number of bytes, including every character of every field contained in the record.

6.2.2 Field 9.002: Image designation character (IDC)

This mandatory two-byte field shall be used for the identification and location of the minutiæ data. The IDC contained in this field shall match the IDC found in the file content field of the Type-1 record.

6.2.3 Field 9.003: Impression type (IMP)

This mandatory one-byte field shall describe the manner by which the dactyloscopic image information was obtained. The ASCII value of the proper code as selected from Table 3.1 shall be entered in this field to signify the impression type.

6.2.4 Field 9.004: Minutiæ format (FMT)

This field shall contain a "U" to indicate that the minutiae are formatted in M1-378 terms. Even though information may be encoded in accordance with the M1-378 standard, all data fields of the Type-9 record must remain as ASCII text fields.

6.2.5 Field 9.126: CBEFF information

This field shall contain three information items. The first information item shall contain the value "27" (0x1B). This is the identification of the CBEFF Format Owner assigned by the International Biometric Industry Association (IBIA) to INCITS Technical Committee M1. The <US> character shall delimit this item from the CBEFF Format Type that is assigned a value of "513" (0x0201) to indicate that this record contains only location and angular direction data without any Extended Data Block information. The <US> character shall delimit this item from the CBEFF Product Identifier (PID) that identifies the "owner" of the encoding equipment. The vendor establishes this value. It can be obtained from the IBIA website (www.ibia.org) if it is posted.

6.2.6 Field 9.127: Capture equipment identification

This field shall contain two information items separated by the <US> character. The first shall contain "APPF" if the equipment used originally to acquire the image was certified to comply with Appendix F (IAFIS Image Quality Specification, January 29, 1999) of CJIS-RS-0010, the Federal Bureau of Investigation's Electronic Fingerprint Transmission Specification. If the equipment did not comply it will contain the value of "NONE". The second information item shall contain the Capture Equipment ID which is a vendor-assigned product number of the capture equipment. A value of "0" indicates that the capture equipment ID is unreported.

6.2.7 Field 9.128: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image. The maximum horizontal size is limited to 65,534 pixels.

6.2.8 Field 9.129: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image. The maximum vertical size is limited to 65,534 pixels.

6.2.9 Field 9.130: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a "2" indicates pixels per centimetre. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

6.2.10 Field 9.131: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the horizontal component of the pixel aspect ratio.

6.2.11 Field 9.132: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

6.2.12 Field 9.133: Finger view

This mandatory field contains the view number of the finger associated with this record's data. The view number begins with "0" and increments by one to "15".

6.2.13 Field 9.134: Finger position (FGP)

This field shall contain the code designating the finger position that produced the information in this Type-9 record. A code between 1 and 10 taken from table 3.2 or the appropriate palm code from table 6.3 shall be used to indicate the finger or palm position.

6.2.14 Field 9.135: Finger quality

The field shall contain the quality of the overall finger minutiæ data and shall be between 0 and 100. This number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutiæ record.

6.2.15 Field 9.136: number of minutiæ

The mandatory field shall contain a count of the number of minutiæ recorded in this logical record.

6.2.16 Field 9.137: Finger minutiæ data

This mandatory field has six information items separated by the <US> character. It consists of several subfields, each containing the details of single minutiae. The total number of minutiae subfields must agree with the count found in field 136. The first information item is the minutiae index number, which shall be initialized to "1" and incremented by "1" for each additional minutia in the fingerprint. The second and third information items are the 'x' coordinate and 'y' coordinates of the minutiae in pixel units. The fourth information item is the minutiae angle recorded in units of two degrees. This value shall be nonnegative between 0 and 179. The fifth information item is the minutiae type. A value of "0" is used to represent minutiae of type "OTHER", a value of "1" for a ridge ending and a value of "2" for a ridge bifurcation. The sixth information item represents the quality of each minutiae. This value shall range from 1 as a minimum to 100 as a maximum. A value of "0" indicates that no quality value is available. Each subfield shall be separated from the next with the use of the <RS> separator character.

6.2.17 Field 9.138: Ridge count information

This field consists of a series of subfields each containing three information items. The first information item of the first subfield shall indicate the ridge count extraction method. A "0" indicates that no assumption shall be made about the method used to extract ridge counts, nor their order in the

record. A "1" indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in four quadrants, and ridge counts for each centre minutia are listed together. A "2" indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in eight octants, and ridge counts for each centre minutia are listed together. The remaining two information items of the first subfield shall both contain "0". Information items shall be separated by the <US> separator character. Subsequent subfields will contain the centre minutiae index number as the first information item, the neighbouring minutiae index number as the second information item, and the number of ridges crossed as the third information item. Subfields shall be separated by the <RS> separator character.

6.2.18 Field 9.139: Core information

This field will consist of one subfield for each core present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the core recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

6.2.19 Field 9.140: Delta information

This field will consist of one subfield for each delta present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the delta recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

7. Type-13 variable-resolution latent image record

The Type-13 tagged-field logical record shall contain image data acquired from latent images. These images are intended to be transmitted to agencies that will automatically extract or provide human intervention and processing to extract the desired feature information from the images.

Information regarding the scanning resolution used, the image size, and other parameters required to process the image, are recorded as tagged-fields within the record.

Table 7: Type-13 variable-resolution latent record layout

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	--

Key for character type: N = Numeric; A = Alphabetic; AN = Alphanumeric; B = Binary

7.1 Fields for the Type-13 logical record

The following paragraphs describe the data contained in each of the fields for the Type-13 logical record.

Within a Type-13 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-13 record, table 5.1 lists the “condition code” as being mandatory “M” or optional “O”, the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the “field size per occurrence” include all character separators used in the field. The “maximum byte count” includes the field number, the information, and all the character separators including the “GS” character.

7.1.1 Field 13.001: Logical record length (LEN)

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-13 logical record. Field 13.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

7.1.2 Field 13.002: Image designation character (IDC)

This mandatory ASCII field shall be used to identify the latent image data contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

7.1.3 Field 13.003: Impression type (IMP)

This mandatory one- or two-byte ASCII field shall indicate the manner by which the latent image information was obtained. The appropriate latent code choice selected from table 3.1 (finger) or table 5.3 (palm) shall be entered in this field.

7.1.4 Field 13.004: Source agency / ORI (SRC)

This mandatory ASCII field shall contain the identification of the administration or organization that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/*agency*.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

7.1.5 Field 13.005: Latent capture date (LCD)

This mandatory ASCII field shall contain the date that the latent image contained in the record was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and unit values of the day in the month. For example, 20000229 represents February 29, 2000. The complete date must be a legitimate date.

7.1.6 Field 13.006: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

7.1.7 Field 13.007: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

7.1.8 Field 13.008: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a "2" indicates pixels per centimetre. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

7.1.9 Field 13.009: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Other-wise, it indicates the horizontal component of the pixel aspect ratio.

7.1.10 Field 13.010: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

7.1.11 Field 13.011: Compression algorithm (CGA)

This mandatory ASCII field shall specify the algorithm used to compress grayscale images.

Table 8 : Compression Codes

Compression Type	Code
No Compression	NONE
Wavelet/Scalar Quantization (IAFIS-IC-0110)	WSQ
JPEG 2000	J2K

7.1.12 Field 13.012: Bits per pixel (BPX)

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of “8” for normal grayscale values of “0” to “255”. Any entry in this field greater than “8” shall represent a grayscale pixel with increased precision.

7.1.13 Field 13.013: Finger / palm position (FGP)

This mandatory tagged-field shall contain one or more the possible finger or palm positions that may match the latent image. The decimal code number corresponding to the known or most probable finger position shall be taken from table 3.2 or the most probable palm position from table 5.3 and entered as a one- or two-character ASCII subfield. Additional finger and/or palm positions may be referenced by entering the alternate position codes as subfields separated by the “RS” separator character. The code "0", for "Unknown Finger", shall be used to reference every finger position from one through ten. The code “20”, for “Unknown Palm”, shall be used to reference every listed palmprint position.

7.1.14 Field 13.014-019: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.15 Field 13.020: Comment (COM)

This optional field may be used to insert comments or other ASCII text information with the latent image data.

7.1.16 Field 13.021-199: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.17 Fields 13.200-998: User-defined fields (UDF)

These fields are user-definable fields. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

7.1.18 Field 13.999: Image data (DAT)

This field shall contain all of data from a captured latent image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, “13.999:” is followed by image data in a binary representation.

Each pixel of uncompressed grayscale data shall normally be quantized to eight bits (256 gray levels) contained in a single byte. If the entry in BPX Field 13.012 is greater or less than “8”, the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the GCA field.

7.2 End of Type-13 variable-resolution latent image record

For the sake of consistency, immediately following the last byte of data from field 13.999 an "FS" separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-13 record.

8. Type-15 variable-resolution palmprint image record

The Type-15 tagged-field logical record shall contain and be used to exchange palmprint image data together with fixed and user-defined textual information fields pertinent to the digitized image. Information regarding the scanning resolution used, the image size and other parameters or comments required to process the image are recorded as tagged-fields within the record. Palmprint images transmitted to other agencies will be processed by the recipient agencies to extract the desired feature information required for matching purposes.

The image data shall be acquired directly from a subject using a live-scan device, or from a palmprint card or other media that contains the subject's palmprints.

Any method used to acquire the palmprint images shall be capable of capturing a set of images for each hand. This set shall include the writer's palm as a single scanned image, and the entire area of the full palm extending from the wrist bracelet to the tips of the fingers as one or two scanned images. If two images are used to represent the full palm, the lower image shall extend from the wrist bracelet to the top of the interdigital area (third finger joint) and shall include the thenar, and hypothenar areas of the palm. The upper image shall extend from the bottom of the interdigital area to the upper tips of the fingers. This provides an adequate amount of overlap between the two images that are both located over the interdigital area of the palm. By matching the ridge structure and details contained in this common area, an examiner can confidently state that both images came from the same palm.

As a palmprint transaction may be used for different purposes, it may contain one or more unique image areas recorded from the palm or hand. A complete palmprint record set for one individual will normally include the writer's palm and the full palm image(s) from each hand. Since a tagged-field logical image record may contain only one binary field, a single Type-15 record will be required for each writer's palm and one or two Type-15 records for each full palm. Therefore, four to six Type-15 records will be required to represent the subject's palmprints in a normal palmprint transaction.

8.1 Fields for the Type-15 logical record

The following paragraphs describe the data contained in each of the fields for the Type-15 logical record.

Within a Type-15 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last

physical field in the record. For each field of the Type-15 record, table 6.1 lists the "condition code" as being mandatory "M" or optional "O", the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the "field size per occurrence" include all character separators used in the field. The "maximum byte count" includes the field number, the information, and all the character separators including the "GS" character.

8.1.1 Field 15.001: Logical record length (LEN)

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-15 logical record. Field 15.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

8.1.2 Field 15.002: Image designation character (IDC)

This mandatory ASCII field shall be used to identify the palmprint image contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

8.1.3 Field 15.003: Impression type (IMP)

This mandatory one-byte ASCII field shall indicate the manner by which the palmprint image information was obtained. The appropriate code selected from table 6.2 shall be entered in this field.

8.1.4 Field 15.004: Source agency/ORI (SRC)

This mandatory ASCII field shall contain the identification of the administration or organization that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/*agency*.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

8.1.5 Field 15.005: Palmprint capture date (PCD)

This mandatory ASCII field shall contain the date that the palmprint image was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and units values of the day in the month. For example, the entry 20000229 represents February 29, 2000. The complete date must be a legitimate date.

8.1.6 Field 15.006: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

8.1.7 Field 15.007: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

8.1.8 Field 15.008: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a "2" indicates pixels per centimeter. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

8.1.9 Field 15.009: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Other-wise, it indicates the horizontal component of the pixel aspect ratio.

8.1.10 Field 15.010: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

Table 9: Type-15 variable-resolution palmprint record layout

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

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min.	max.	
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	--

Table 10 : Palm Impression Type

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 Field 15.011: Compression algorithm (CGA)

This mandatory ASCII field shall specify the algorithm used to compress grayscale images. An entry of "NONE" in this field indicates that the data contained in this record is uncompressed. For those images that are to be compressed, this field shall contain the preferred method for the compression of tenprint fingerprint images. Valid compression codes are defined in table A7.1.

8.1.12 Field 15.012: Bits per pixel (BPX)

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of "8" for normal grayscale values of "0" to "255". Any entry in this field greater than or less than "8" shall represent a grayscale pixel with increased or decreased precision respectively.

Table 11: Palm Codes, Areas & Sizes

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28387	139.7	203.2
Right Full Palm	21	28387	139.7	203.2
Right Writer s Palm	22	5645	44.5	127.0
Left Full Palm	23	28387	139.7	203.2
Left Writer s Palm	24	5645	44.5	127.0
Right Lower Palm	25	19516	139.7	139.7
Right Upper Palm	26	19516	139.7	139.7
Left Lower Palm	27	19516	139.7	139.7
Left Upper Palm	28	19516	139.7	139.7
Right Other	29	28387	139.7	203.2
Left Other	30	28387	139.7	203.2

8.1.13 Field 15.013: Palmprint position (PLP)

This mandatory tagged-field shall contain the palmprint position that matches the palmprint image. The decimal code number corresponding to the known or most probable palmprint position shall be taken from table 6.3 and entered as a two-character ASCII subfield. Table 6.3 also lists the maximum image areas and dimensions for each of the possible palmprint positions.

8.1.14 Field 15.014-019: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.15 Field 15.020: Comment (COM)

This optional field may be used to insert comments or other ASCII text information with the palmprint image data.

8.1.16 Field 15.021-199: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.17 Fields 15.200-998: User-defined fields (UDF)

These fields are user-definable fields. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

8.1.18 Field 15.999: Image data (DAT)

This field shall contain all of the data from a captured palmprint image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, “15.999:” is followed by image data in a binary representation. Each pixel of uncompressed grayscale data shall normally be quantized to eight bits (256 gray levels) contained in a single byte. If the entry in BPX Field 15.012 is greater or less than 8, the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the CGA field.

8.2 End of Type-15 variable-resolution palmprint image record

For the sake of consistency, immediately following the last byte of data from field 15.999 an “FS” separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-15 record.

8.3 Additional Type-15 variable-resolution palmprint image records

Additional Type-15 records may be included in the file. For each additional palmprint image, a complete Type-15 logical record together with the “FS” separator is required.

APPENDIX 1 ASCII Separator Codes

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

APPENDIX 2 Calculation of Alpha-Numeric Check Character

For TCN and TCR (Fields 1.09 and 1.10):

The number corresponding to the check character is generated using the following formula:

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

Where YY and SSSSSSSS are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

For CRO (Field 2.010)

The number corresponding to the check character is generated using the following formula:

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

Where YY and NNNNNN are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

[1] This is the position as defined in the ASCII standard.

Check Character Look-up Table

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	

APPENDIX 3 Character Codes

7-bit ANSI code for information interchange

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	{	|	}	~			

APPENDIX 4 Transaction Summary

Type 1 Record (mandatory)

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
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

Under the Condition Column:
O = Optional; M = Mandatory; C = Conditional if transaction is a response to the origin agency

Type 2 Record (mandatory)

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

Identifier	Field Number	Field Name	CPS/ PMS	MPS/ MMS	SRE	ERR
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	-	-

Under the Condition Column:
O = Optional; M = Mandatory; C = Conditional if data is available
*) = if the transmission of the data is in accordance with national law (not covered by the Treaty)

APPENDIX 5 Type-1 Record Definitions

Table A.5: Type-1 Record Definitions

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

Under the Condition Column: O= Optional, M= Mandatory, C= Conditional
Under the Character Type Column: A= Alpha, N= Numeric, B= Binary
1* allowed characters for agency name are ["0..9", "A..Z", "a..z", "_", ".", " ", "-"]

APPENDIX 6 Type-2 Record Definitions

Table A.6.1: CPS- and PMS-Transaction

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}
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}

Table A.6.2: SRE-Transaction

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: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}

Table A.6.3: ERR-Transaction

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}
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC -1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {GS}

Table A.6.4: MPS- and MMS-Transaction

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}

Under the Condition Column: O= Optional, M= Mandatory, C= Conditional
Under the Character Type Column: A= Alpha, N= Numeric, B= Binary
1* allowed characters are ["0..9", "A..Z", "a..z", "_", ".", " ", "-", ","]

APPENDIX 7 Grayscale Compression Codes

A.7.1 Compression Codes

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

APPENDIX 8 Mailspecification

To improve the internal workflow the mailsubject of a PRUEM transaction has to be filled with the country code (CC) of the Party that send the message and the Type of Transaction (TOT Field 1.004).

Format: CC/*type of transaction*
Example: "DE/CPS"

The mailbody can be empty.

The specification of the encryption/signing and the used S/MIME Version will follow as soon as possible in this Appendix, after clarify this points with the DNA Technical Work Group.

Annex B.2

Maximum Number of candidates accepted for verification

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

Search types:

TP/TP: ten-print against ten-print
LT/TP: fingerprint latent against ten-print
LP/PP: palmprint latent against palmprint
TP/UL: ten-print against unsolved fingerprint latent
LT/UL: fingerprint latent against unsolved fingerprint latent
PP/ULP: palmprint against unsolved palmprint latent
LP/ULP: palmprint latent against unsolved palmprint latent

Annex B.3

Maximum research capacities per day for dactyloscopic data of identified persons

	BE	NL	LU	AT	FR	ES	DE
BE	-	20	20	20	20	20	20
NL	20	-	20	20	16	16	24
LU	4	4	-	20	4	4	4
AT	20	20	20	-	60	60	100
FR	144	144	144	60	-	144	144
ES	120	120	120	60	120	-	120
DE	120[1)]	120[1)]	120[1)]	100	120[1)]	120[1)]	-
	428	**428**	**444**	**280**	**300**	**364**	**412**

[1)] estimated throughput for 2007: 60 TP/TP per day

Annex B.4

Maximum research capacities per day for dactyloscopic traces

	BE	NL	LU	AT	FR	ES	DE
BE	-	6	6	6	10	2	6
NL	6	-	6	6	2	2	8
LU	1	1	-	6	1	1	1
AT	6	6	6	-	15	15	30
FR	43	43	43	15	-	43	43
ES	18	18	18	15	18	-	18
DE	40 [1)]	40 [1)]	40 [1)]	30	40 [1)]	40 [1)]	-
	114	**114**	**119**	**78**	**86**	**103**	**106**

[1)] estimated throughput for 2007: 20 LP/TP per day

Annexes C

Automated searching for vehicle registration data

Annex C.1

Common data-set for automated search of vehicle registration data

1. Definitions

For each element in the data set as described in the next chapter, an indication is given whether the element is especially allocated by the Parties and whether the element is mandatory or optional when the exchange is used for the purposes of Article 12 of the Treaty.

The definitions of mandatory data elements and optional data elements are as follows:

Mandatory (M):
The data element has to be communicated when the information is available in one's national register. Therefore there is an **obligation** to exchange the information **when available**.

Optional (O):
The data element may be communicated when the information is available in one's national register. Therefore there is **no obligation** to exchange the information even when the information is available.

An indication (Y) is given for each element in the data set whether the element is specifically indicated by the Parties in relation with the Treaty.

2. Vehicle/Owner/Holder Inquiry

2.1 Triggers for the Inquiry

There are two different ways to search for the information as defined in the next paragraph:

1. By Chassis Number (VIN), Reference Date and Time (optional);
2. By License Number, Nature of the vehicle/EU Category Code (optional), Reference Date and Time (optional); in Luxembourg more than one vehicle can be returned when the inquiry is done by Licence Number.

By means of these search criteria, information related to one and sometimes more vehicles will be returned. If information for only one vehicle has to be returned, all the items are returned in **one** response. If more than one vehicle is found, the Party itself can determine which items will be returned; all items or only the items to refine the inquiry (e.g. because of privacy reasons as in UK and Germany, or because of performance reasons).

The items, necessary to refine the inquiry are pictured in paragraph 2.2.1. In paragraph 2.2.2 the complete information set is described.

When the inquiry is done by Chassis Number, Reference Date and Time, the inquiry can be done in **one or all** of the participating countries.

When the inquiry is done by License Number, Reference Data and Time, the inquiry has to be done in **one specific** Party.

Normally the actual Date and Time is used to make an inquiry, but it's possible to do an inquiry with a Reference Date and Time in the past. When an inquiry is made with a Reference Date and Time in the past and historical information is not available in the register of the specific Party, the actual information can be returned with an indication that the information is actual information.

2.2 Data set

2.2.1 Items to be returned necessary for the refinement of the inquiry

Item	M/O[2]	Remarks	Prüm Y/N[3]
Data relating to vehicles			
Licence number	M		**Y**
Chassis number / VIN	M		**Y**
Party of registration	M		**Y**
Make	M	(D.1[4]) 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**

2.2.2 Complete data set

Item	M/O[5]	Remarks	Prüm Y/N
Data relating to holders of the vehicle		**(C.1[6])**	
Registration holders' (company) name	M	(C.1.1.) separate fields will be used for first name(s), 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, Party 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**
ID Number	O	An identifier that uniquely identifies the person or the company.	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**
Address	M	(C.2.3)	**Y**

[2] M = mandatory when available in national register, O = optional
[3] All the attributes specifically allocated by the Parties are indicated with Y.
[4] Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999
[5] M = mandatory when available in national register, O = optional
[6] Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

Item	M/O[5]	Remarks	Prüm Y/N
Gender	M	male, female	**Y**
Date of birth	M		**Y**
Legal entity	M	individual, association, company, firm etc.	**Y**
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Data relating to vehicles			
Licence number	M		**Y**
Chassis number / VIN	M		**Y**
Party 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) vehicle document date	**Y**
End date registration	M		**Y**
Status	M	scrapped, stolen, exported, error notification	**Y**
Status date	M		**Y**
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. In Luxembourg two separate vehicle registration document ID's are used.	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**

Annex C.2

Data Security

1. Overview

The Eucaris software application connects all Parties in a mesh network where each Party communicates directly to another Party. There is no central component needed for the communication to be established. The application handles secure communication to the other Parties and communicates to the back-end legacy systems of Parties using XML. Parties exchange messages by directly sending them to the recipient. The data center of a Party is connected to the Testa II network of EU.

The XML-messages sent over the network are encrypted. The technique to encrypt these messages is SSL. The messages sent to the back-end are plain text XML-messages since it is assumed the connection between the application and the back-end is in a protected environment.

Finally, a client application is provided which can be used within a Party to query their own register or other Parties. The clients will be identified by means of user-id/password or a client certificate. The connection to a user may be encrypted. However, this is the responsibility of each individual Party.

2. Security Features related to message exchange

The security design is based on a combination of HTTPS and XML signature. This alternative uses XML-signature to sign all messages sent so the server and can authenticate the sender of the message by checking the signature. 1-sided SSL (only a server certificate) is used to protect the confidentiality and integrity of the message in transit and provides protection against deletion and insertion attacks.

The XML-signature can be implemented in several ways.

The chosen approach is to use XML Signature as part of the Web Services Security (WSS). WSS specifies how to use XML-signature. Since WSS builds upon the SOAP standard, it is logical to adhere to the SOAP standard as much as possible. This requires changes to the XML-messages specified with respect to addressing, error handling etc.

The use of XML-signature and HTTPS with server certificate (1-sided SSL) combines the best properties of XML-signature on one side and HTTPS on the other side. No additional measures are needed to protect against deletion/replay attacks. Instead of bespoke software development to implement 2-sided SSL, XML-signature is implemented. Using XML-signature is closer to the web services roadmap than 2-sided SSL and therefore more strategic.

3. Security features not related to message exchange

3.1 Authentication of users

The users of the Eucaris web application authenticate themselves using a username and password. Since standard Windows authentication is used, Parties can enhance the level of authentication of users if needed by using client certificates.

3.2 User roles

The Eucaris software application supports different user roles. Each cluster of services has its own authorization. E.g. (exclusive) users of the "Treaty of Eucaris"- functionality" may not use the "Treaty of Prüm"- functionality". Administrator services are separated from the regular end-user roles.

3.3 Logging and tracing of message exchange

Logging of all message types is facilitated by the Eucaris software application. An administrator function allows the national administrator to determine which messages are logged: requests from end-users, incoming requests from other Parties, provided information from the national registers, etc.

The application can be configured to use an internal database for this logging, or an external (Oracle) database. The decision on what messages have to be logged clearly depends on logging facilities elsewhere in the legacy systems and connected client applications.

The header of each message contains information on the requesting Party, the requesting organization within that Party and the user involved. Also the reason of the request is indicated.

By means of the combined logging in the requesting and responding Party complete tracing of any message exchange is possible (e.g. on request of a citizen involved).

Logging is configured through the Eucaris web client (menu Administration, Logging configuration). The logging functionality is performed by the Core System. When logging is enabled, the complete message (header and body) is stored in one logging record. Per defined service, and per message type that passes along the Core System, the logging level can be set.

Logging Levels
The following logging levels are possible:
Private – Message is logged: The logging is NOT available to the extract logging service run by the Secretary State but is available on a national level only, for audits and problem solving.
None – Message is not logged at all.

Message Types

Information exchange between Parties consists of several messages, of which a schematic representation is given in the figure below.

The possible message types (in the figure shown for the Eucaris Core System of Party X) are the following:

1. Request to Core System_Request message by Client
2. Request to Other Party Request message by Core System of this Party
3. Request to Core System of this Party_Request message by Core System of other Party
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 Party_Request message by Core System of this Party
8. Response from Core System of this Party_Request message by other Party
9. Response from Legacy Register_Request message by Core System
10. Response from Core System_Request message by Legacy Register

The following information exchanges are shown in the figure:

- Information request from this Party (X) to another Party (Y) – blue arrows. This request and response consists of message types 1, 2, 7 and 6, respectively.
- Information request from another Party (Z) to this Party (X) – red arrows. This request and response consists of message types 3, 4, 9 and 8, respectively.
- Information request from the legacy register to its core system (this route also includes a request from a custom client behind the legacy register) – green arrows. This kind of request consists of message types 5 and 10.

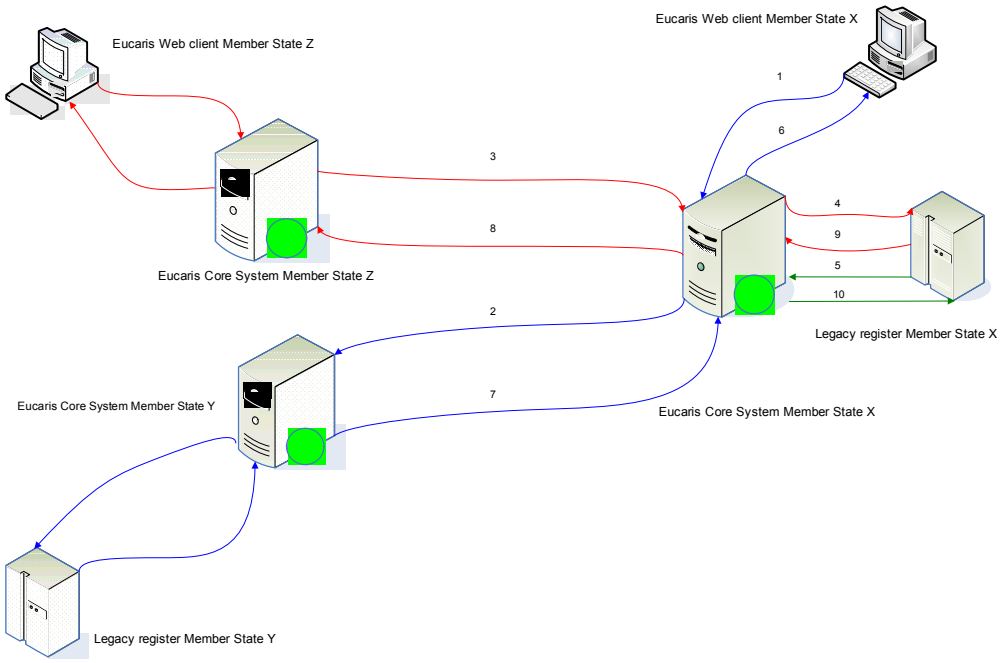


Figure : Message types for logging

3.4 Hardware Security Module

A Hardware Security Module is not used.

A Hardware Security Module (HSM) provides good protection for the key used to sign messages and to identify servers. This adds to the overall level of security but an HSM is expensive to buy/maintain and there are no requirements to decide for a FIPS 140-2 level 2 or level 3 HSM. Since a closed network is used that mitigates threats effectively, it is decided not to use an HSM initially. If an HSM is necessary e.g. to obtain accreditation, it can be added to the architecture.

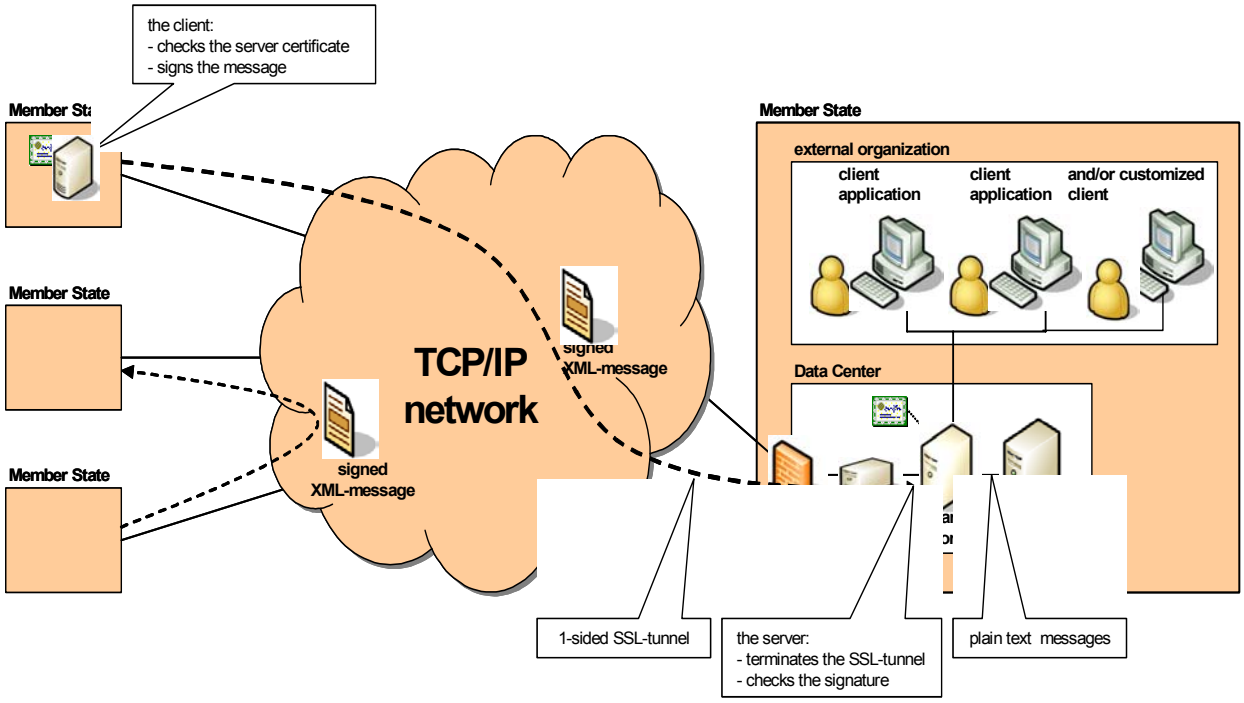
Annex C.3

Technical conditions of the data exchange

1. General description of the EUCARIS application

1.1 An overview

The Eucaris application connects all participating Parties in a mesh network where each Party communicates directly to another Party. There is no central component needed for the communication to be established. The Eucaris application handles secure communication to the other Parties and communicates to the back-end legacy systems of Parties using XML. The following picture visualizes this architecture.



Parties exchange messages by directly sending them to the recipient. The data center of a Party is connected to the network used for the message exchange (Testa). To access the Testa network, Parties connect to Testa via their national gate. It is assumed that a firewall is used to connect to the network

and that a router connects the Eucaris application to the firewall. Depending on the alternative chosen to protect the messages, a certificate is used either by the router or by the Eucaris application.

The XML-messages sent over the network are encrypted. The technique to encrypt these messages is SSL. The messages sent to the back-end are plain text XML-messages since it is assumed the connection between Eucaris and the back-end is in a protected environment.

Finally, a client application is provided which can be used within a Party to query its own register or other Parties. The client application connects to Eucaris. The clients will be identified by means of user-id/password or a client certificate. The connection to a user in an external organization (e.g. police) may be encrypted. However, this is the responsibility of each individual Party.

1.2 Scope of the system

The scope of the Eucaris system is limited to the processes involved in the exchange of information between the Registration Authorities in the Parties and a basic presentation of this information. Procedures and automated processes in which the information is to be used (e.g. administrative or enforcement processes), are outside the scope of the system.

Parties can choose either to use the Eucaris client functionality or to realise their own customized client application. In the table below, it is described which aspects of the Eucaris system are mandatory to use and/or prescribed and which are optional to use and/or free to determine by the Parties.

EUCARIS aspects	M/O[7]	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 Parties. The following functionality is offered by the core: ▪ Encrypting and signing of the messages; ▪ Checking of the identity of the sender; ▪ Authorization of Parties and local users; ▪ Routing of messages; ▪ Queuing of asynchronous messages if the recipient service is temporally unavailable; ▪ Multiple country inquiry functionality; ▪ Logging of the exchange of messages; ▪ Storage of incoming messages
Client application	O	In addition to the core application the EUCARIS II client application can be used by a Party. When applicable, the core and client application is 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.

[7] M = mandatory to use or to comply with O = optional to use or to comply with

EUCARIS aspects	M/O[7]	Remark
Message specifications	M	Every Party has to comply with the message specifications as set by the EUCARIS organisation and the present Implementing Agreement and its Annexes c. The specifications can only be changed by the EUCARIS organisation in consultation with the Parties.
Operation and Support	M	The acceptation of new Parties or new functionality is under auspices of the EUCARIS organisation. Monitoring and help desk functions are managed centrally by an appointed Party.

2. Non Functional Requirements

2.1 Generic functionality

In this section the main generic functions have been described in general terms.

Nr.	Description
1.	The system allows the Registration Authorities of the Parties to exchange request and response messages in an interactive way.
2.	The system contains a client application, enabling end-users to send their requests and presenting the response information for manual processing.
3.	The system facilitates 'broadcasting', allowing a Party to send a request to all other Parties. The incoming responses are consolidated by the core application in one response message to the client application (this functionality is called a 'Multiple Country Inquiry').
4.	The system is able to deal with different types of messages. User roles, authorization, routing, signing and logging are all defined per specific service.
5.	The system allows the Parties to exchange batches of messages or messages containing a large number of requests or replies. These messages are dealt with in an asynchronous way.
6.	The system queues asynchronous messages if the recipient Party is temporarily unavailable and guarantees the deliverance as soon as the recipient is up again.
7.	The system stores incoming asynchronous messages until they can be processed.
8.	The system gives only access to Eucaris applications of other Parties, not to individual organisations within those other Parties, i.e. each Registration Authority acts as the single gateway between its national end-users and the corresponding Authorities in the other Parties.
9.	It is possible to define users of different Parties on one Eucaris server and to authorize them following the rights of that Party.
10.	Information on the requesting Party, organisation and end user are included in the messages.
11.	The system facilitates logging of the exchange of messages between the different Parties and between the core application and the national registration systems.
12.	The system allows a specific secretary, which is an organisation or Party explicitly appointed for this task, to gather logged information on messages sent/received by all the participating Parties, in order to produce statistical reports.

Nr.	Description
13.	Each Party indicates itself what logged information is made available for the secretary and what information is 'private'.
14.	The system allows the National Administrators of each Party to extract statistics of use.
15.	The system enables addition of new Parties through simple administrative tasks.

2.2 Usability

Nr.	Description
16.	The system provides an interface for automated processing of messages by back-end systems/legacy and enables the integration of the user interface in those systems (customised user-interface).
17.	The system is easy to learn, self explanatory and contains help-text.
18.	The system is documented to assist Parties in integration, operational activities and future maintenance (e.g. reference guides, functional/technical documentation, operational guide,….).
19.	The user interface is multi-lingual and offers facilities for the end-user to select a preferred language.
20.	The user interface contains facilities for a Local Administrator to translate both screen-items and coded information to the national language.

2.3 Reliability

Nr.	Description
21.	The system is designed as a robust and dependable operational system which is tolerant to operator errors and which will recover cleanly from power cuts or other disasters. It must be possible to restart the system with no or minimal loss of data.
22.	The system must give stable and reproducible results.
23.	The system has been designed to function reliably. It is possible to implement the system in a configuration that guarantees an availability of 98% (by redundancy, the use of back-up servers etc.) in each bilateral communication.
24.	It is possible to use part of the system, even during failure of some components (if Party C is down, Parties A and B are still able to communicate). The number of single points of failure in the information chain should be minimised.
25.	The recovery time after a severe failure should be less than one day. It should be possible to minimise down-time by using remote support e.g. by a central service desk.

2.4 Performance

Nr.	Description
26.	The system can be used 24x7. This time-window (24x7) is then also required from the Parties legacy systems.
27.	The system responds rapidly to user requests irrespective of any background tasks. This is also required from the Parties legacy systems to ensure acceptable response time. An overall response time of 10 seconds maximum for a single request is acceptable.

Nr.	Description
28.	The system has been designed as a multi-user system and in such a way that background tasks can continue while the user performs foreground tasks.
29.	The system has been designed to be scaleable in order to support the potential increase of number of messages when new functionality is added or new organisations or Parties are added.

2.5 Security

Nr.	Description
30.	The system is suited (e.g. in its security measures) for the exchange of messages containing privacy-sensitive personal data (e.g. car owner/holders or driving licence holders), classified as EU restricted.
31.	The system is maintained in such a way that unauthorised access to the data is prevented.
32.	The system contains a service for the management of the rights and permissions of national end-users.
33.	Parties are able to check the identity of the sender (at Party level), by means of XML-signing.
34.	Parties must explicitly authorise other Parties to request specific information, enabling the exchange of information both within and outside the scope of a specific treaty or directive.
35.	The system provides at application level a full security and encryption policy compatible with the level of security required in such situations. Exclusiveness and integrity of the information is guaranteed by the use of XML-signing and encryption by means of SSL-tunnelling.
36.	All exchange of messages can be traced by means of logging.
37.	Protection is provided against deletion attacks (a third party deletes a message) and replay or insertion attacks (a third party replays or inserts a message).
38.	The system makes use of certificates of a Trusted Third Party (TTP).
39.	The system is able to handle different certificates per Party, depending on the type of message or service.
40.	The security measures at application level are sufficient to allow the use of non accredited networks.
41.	The system is able to use novice security techniques such as an XML-firewall.

2.6 Adaptability

Nr.	Description
42.	The system is extensible with new messages and new functionality (e.g. name matching algorithms). The costs of adaptations are minimal. Due to the centralised development of application components.
43.	MS are able to define new message types for bilateral use. Not all Parties are required to support all message types.

2.7 Support and Maintenance

Nr.	Description
44.	The system provides monitoring facilities for a central service-desk and/or operators concerning the network and servers in the different Parties.
45.	The system provides facilities for remote support by a central service-desk.
46.	The system provides facilities for problem analysis.
47.	The system can be expanded to new Parties.
48.	The application can easily be installed.
49.	The system provides a permanent testing and acceptance environment.
50.	The annual costs of maintenance and support has been minimised by adherence to market standards and by creating the application in such a way that as little support as possible from a central service-desk is required.

2.8 Design requirements

Nr.	Description
51.	The system is designed and documented for an operational lifetime of many years.
52.	The system has been designed in such a way that it is independent of the network provider.
53.	The system is compliant with the existing HW/SW in the Parties by interacting with those registration systems using standard web service technology (XML, HTTP, Web services, WSS).

2.9 Applicable standards

Nr.	Description
54.	The system is compliant with data protection issues as stated in Regulation EC 45/2001 (articles 21, 22 & 23) and Directive 95/46/EC.
55.	The system complies with the IDA Standards [doc-1].
56.	The system supports UTF8.

Annex C.4

List of contact points for incoming requests

Country	Contact point	Telephone number (for operational contact)	Fax number (for operational contact)	e-mail (for operational contact)
Austria	Bundeskriminalamt Österreich (Austrian Criminal Intelligence Service)	**+43 1 24836 85026**	**+43 1 24836 951135**	**BMI-II-BK-SPOC@bmi.gv.at**
Belgium	DIV "Dienst Inschrijvingen" (Vehicle Registration)	**+ 32 2 2773 792 (DIV) + 32 2 2773 777 (ICT)**	**+ 32 2 277 40 22 (DIV) + 32 2 277 40 04**	**Help.div@mobilit.fgov.be (DIV) Help.ict@mobilit.fgov.be (ICT)**
France	SCCOPOL "Section Centrale de Coopération policière" (Criminal Investigation Police)	**+ 33 (0) 1 40 97 88 73**	**+ 33 (0) 1 40 97 82 48**	**dcpj-dri-pcc@interieur.gouv.fr**
Germany	KBA "Kraftfahrt-Bundesamt" (Vehicle Registration)	**+ 49 461 316 2050**	**+ 49 461 316 2942**	**pruem@kba.de**
Luxembourg	Centre Informatique de la Police (Police)	**+ 35 2 4997 2346**	**+ 35 2 4997 2398**	**cin@police.etat.lu**
Netherlands (The)	RDW "Rijksdienst Wegverkeer" (Vehicle Registration)	**+ 31 598 693 369**	**+ 31 503 656 462**	**servicedesk@rdw.nl**
Spain	Secretaria de Estado de Seguridad (Ministry of Interior)	**+34915371883 +34915371884 +34915372056 +34915372057 +34915372058**	**+34913191228 +34913191645 +34913197389**	**cepic@ses.mir.es**

Annexes D

Police cooperation

Annex D.1

Procedures and contact points for the setting up of joint operations

Parties which do not use or work with specified procedures where the intervention of a contact point is necessary for setting up joint operations pursuant to article 24 of the Treaty give relevant contact points for the setting up of joint operations mentioned below.

AUSTRIA

National contact point according to point 14.2 of the Implementing Agreement:

During office hours:
Federal Ministry of the Interior, General Directorate for Public Security,
Sub-Department II/2/a
Phone: +431-53126-3411
Fax: +431-53126-10-8638
e-mail: bmi-II-2-a@bmi.gv.at

Outside office hours:
Federal Ministry of the Interior, Division II – General Directorate for Public Security, Operations and Crisis Coordination Centre
Phone: +431-53126-3200 or -3775
Fax: +431-53126-3120
e-mail: bmi-II-EKC-Permanenzdienst@bmi.gv.at

BELGIUM

1. Joint patrols and joint controls

There is no formal procedure that needs to be followed when setting up a joint patrol or joint control. It suffices that the operational chiefs of the services involved (in Belgium: the corps chief of the Local Police or the chief of unit of the Federal Police) come to a verbal or written agreement. If one does not know how to get in touch with the Belgian operational chief, one should take contact with the national contact point:

DAO (Directorate of operations concerning administrative police – Officer on duty)
Blok G, Fritz Toussaintstraat 47
1050 Elsene
Tel.: + 32 2 642.63.80
Fax: + 32 2 646.49.40
E-mail: dga-dao@skynet.be.

The operational chiefs make sure that every officer taking part in the operation is well informed about the mission and the competencies. If necessary, a meeting will be organised to this purpose.

2. Other joint operations

Other joint operations are only possible on request. All requests to the Belgian Police have to be made by means of the request form below and have to be sent to the national contact point:

DAO (Directorate of operations concerning administrative police – Officer on duty)
Blok G, Fritz Toussaintstraat 47
1050 Elsene
Tel.: + 32 2 642.63.80
Fax: + 32 2 646.49.40
E-mail: dga-dao@skynet.be.

The competent authority in Belgium will immediately take a decision concerning the request. The decision is sent as quickly as possible in writing to the competent authority of the requesting Party.

When carrying out the joint operation, the cross-border official is in possession of a summary list of the means and material he brought. He submits it on request to the competent authority of the host state.

FRANCE

	Organisation	Municipality	Telephone number Fax number E-mail
AUSTRIA	CCPD	Kehl	Tel : 0049.7851.8895-0 Fax : 03 90 23 13 69 E-mail: mailto:centro.lz@1.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)

	Organisation	Municipality	Telephone number Fax number E-mail
NETHERLANDS	CCPD	Tournai	Tel : 00 32 69 68 26 10 Fax :00 32 69 68 26 21 E-mail : ccpd-tournai.dzaf-59@interieur.gouv.fr
GERMANY	CCPD	Kehl	Tel : 0049.7851.8895-0 Fax : 03 90 23 13 69 E-mail: mailto:centro.lz@1.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)
SPAIN	CCPD	Hendaye	Tel : 05 59 20 93 60 Fax: 05 59 20 59 34 E-mail : ccpd-hendaye@interieur.gouv.fr
	CCPD	Le Perthus	Tel : 04 68 83 79 00 Fax : O4 68 83 79 10 Tel : 05 59 20 93 60 Fax : 05 59 20 59 34 E-mail : ccpd-hendaye@interieur.gouv.frccpd-sec.le-perthus-66@intermel.si.mi
	CCPD	Canfranc le Somport	Tel : 05 59 39 04 85 Fax : 05 59 36 18 15 E-mail : ccpd.canfranc@interieur.gouv.fr
	CCPD	Melles Pont du Roy	Tel : 05 61 94 68 40 Fax : 05 61 94 68 48 E-mail : ccpd.melles@interieur.gouv.fr
BELGIUM	CCPD	Tournai	Tel : 00 32 69 68 26 10 Fax :00 32 69 68 26 21 E-mail : ccpd-tournai.dzaf-59@interieur.gouv.fr
LUXEMBURG	CCPD	Luxembourg	Tel : 03 82 54 94 30 ou +352 26 124 300 Fax : 03 82 54 94 39 ou +352 26 124 199 E-mail : fr@bccp.etat.lu

GERMANY

1. Introduction to Article 24

Generally, all offices of the Länder police forces and of the Federal Police may be responsible for joint operations.

However, this only applies,
- if there are no regulations in place in bilateral and multilateral treaties governing joint operations that are more specific, and
- if the joint operations do not have a direct cross-border link (e.g. operation of Spanish officers in Germany).

If with respect to a joint operation there is no more specific, contractual rule in place and if there is no direct cross-border link, these exceptional cases require the consent of the Federal Ministry of the Interior and/or the affected interior ministries of the Länder.

Paras 1 and 2 of Article 24 are linked with one another in an inseparable context. For all **measures** carried out pursuant to para 1, **consent** must invariably be obtained under para 2 about the scope of the transfer of sovereign powers, operational modalities and the right of managing the operation which shall rest with the officials from the host state.

2. Ad Artice 24 (1) – „authorities designated by the Contracting Parties"

Examples of joint operations:

Above all "not time-critical situations" ("Zeitlagen") (in the run-up to events that can be planned) such as joint patrols in the border region, joint patrols on the occasion of special events (e.g. Lower-Saxons' Day), joint controls (e.g. to fight international crime such as drug crimes, trafficking in human beings, property crimes organized by gangs (referred to as checks "irrespective of whether there is a specific suspicion"), joint intelligence measures / warnings to potential offenders / fan escorts in the run-up to football matches or other major events.

The principles referred to in 1. shall apply.

Allgemeine Kontaktstellen, auch für andere Vertragsparteien:	
(direkte grenzüberschreitende Zusammenarbeit)	
Bundespolizei Bundespolizeidirektion Roonstr. 13 D-56068 Koblenz	Tel.: +49 (0) 261 399 – 0 Tel.: +49 (0) 261 399 – 250 Fax.: +49 (0) 261 399 – 218 Mail: bpold@polizei.bund.de

3. Ad Article 24(2) sentence 1 – "consent on exercise of sovereign powers"

Co-operation where consent by the Federal Ministry of the Interior must be obtained:

Bundesministerium des Innern
- für das Bundeskriminalamt:
  Abteilung Polizeiangelegenheiten;
  Terrorismusbekämpfung
- für die Bundespolizei:
  Abteilung für Angelegenheiten der
  Bundespolizei

Alt-Moabit 101D
D-10559 Berlin

Tel.: +49 (0) 1888 681-1077
Fax.: +49 (0) 1888 681-2926
Mail: poststelle@bmi.bund.de

Tel.: +49 (0) 1888 681-0
Fax: +49 (0) 1888 681-1829
Mail: poststelle@bmi.bund.de

Co-operation where consent must be obtained from a Land interior ministry. In the following you will find the Bündesländer, which share borders with other Prüm Contracting Parties

Niedersachsen (NI)
Niedersächsisches Ministerium für Inneres und Sport
Lavesallee 6
D-30169 Hannover

Tel.: +49 (0) 511 120-6112
Fax.: +49 (0) 511 120-6150
Mail: kvl@mi.niedersachsen.de

Nordrhein-Westfalen (NW)
Innenministerium Nordrhein-Westfalen
- Lagezentrum –
Haroldstraße 5
40190 Düsseldorf

Tel.: +49 (0)211 871 3340/3341/3342/3343/3344
Fax.: +49 (0)211 871 3231
Mail: lagezentrum@im.nrw.de

Rheinland-Pfalz (RP)
Ministerium des Innern und für Sport
- Lagezentrum -
Schillerplatz 3-5
55116 Mainz

Tel.: +49 (0)6131 16 3599
Fax.: +49 (0)6131 16 3600
Mail: lagezentrum@ism.rlp.de

Saarland (SL)
Ministerium für Inneres, Familie, Frauen und Sport
Leitstelle, Lagezentrum-
c/o Landespolizeidirektion
Mainzer Str 134 -136
66121 Saarbrücken

Tel.: +49 (0) 681 962-1260 bis 1263
Fax.: +49 (0) 681 962-1265
Mail: lagezentrum@innensaarland.de

Baden-Württemberg (BW)
Innenministerium Baden-Württemberg
Lagezentrum
Dorotheenstraße 6
70173 Stuttgart

Tel.: +49 (0)711 231 3333
Fax.: +49 (0)711 231 3399
Mail: lagezentrum@im.bwl.de

Bayern (BY) Bayerisches Staatsministerium des Innern - Lagezentrum - Odeonsplatz 3 D-80335 München	Tel.: 0049 (0) 89 2192-20 Fax: 0049 (0) 89 2192-2587 Mail: stmi.lzby@polizei.bayern.de
Bundesländer, which do not share a border with a Prüm Contracting Party	
Brandenburg (BB) Ministerium des Innern des Landes Brandenburg Lageszentrum der Polizei Henning-von-Treskow-Str. 9-13 14467 Potsdam	Tel.: +49 331 866 2871 Fax.: +49 331 866 2879 Mail: lagezentrum@mi.brandenburg.de
Berlin (BE) Senatsverwaltung für Inneres Lagezentrum Berlin Platz der Lüftbrücke 6 12096 Berlin	Tel.: +49 30 466 490 7210 Fax.: +49 30 466 490 7299 Mail: izberlin@seninn.verwalt-berlin.de
Bremen (HB) Lagezentrum M Polizei Bremen In der Vahr 78 28329 Bremen	Tel.: +49 421 362 1854 or 1754 Fax.: +49 421 362 1859 Mail: Lagezentrum@polizei.bremen.de
Hessen (HE) Hessisches Ministerium des Inneres und für Sport LAGEZENTRUM Friedrich-Ebert-Allee 12 D-65185 Wiebaden	Tel.: +49 611 353 2150 Fax.: +49 611 353 1706 Mail: lzhessen@hmdi.hessen.de
Hamburg (HH) Behörde für Inneres Polizei Hamburg Führungs-und Lagedienst Bruno-Georges-Platz 1 22297 Hamburg	Tel.: +49 40 4286 66055 Fax.: +49 40 4286 66049 Mail: FLDI-FLD2@POLIZEI.HAMBURG.DE
Mecklenburg-Vorpommern (MV) Innenministerium Mecklenburg-Vorpommern Arsenal am Pfaffenteich Lagezentrum Alexandrinenstrasse 1 19055 Schwerin	Tel.: +49 385 588 2471 (bis -2479) Fax.: +49 385 588 2480 (oder 2481) Mail: lagezentrum@im.mv-regierung.de
Schleswig-Holstein (SH) Landespolizeiamt Gemeinsames Lage- und Führungszentrum Mühlen 166 24116 Kiel	Tel.: +49 431 160 61111 Fax.: +49 431 160 61199 Mail: lob.gifz@polizei.landsh.de

Sachsen (SN)
Sächsisches Staatsministerium des Innern
Landespolizeipräsidium
Lagezentrum
01095 Dresden

Tel.: +49 351 564 3775 oder 3776
Fax.: +49 351 564 3779
Mail: Platz2.Lagezentrum@smi.sachsen.de

Sachsen-Anhalt (ST)
Ministerium des Innern
des landes Sachsen-Anhalt
Lagezentrum
Halberstädter Str 2/Am Platz des 17. Juni
39112 Magdeburg

Tel.: +49 391 567 5292
Fax.: +49 391 567 5290
Mail: lagezentrum@mi.lsa-net.de

Thüringen (TH)
Thüringer Innenministerium
Abteilung 4
-Lagezentrum-
Andreasstrasse 38
99084 Erfurt

Tel.: +49 361 37 93 616
Fax.: +49 361 37 93 686
Mail: Lagezentrum@tim.thueringen.de

LUXEMBOURG

The Luxembourg law does not provide for a formal procedure to be accomplished for the setting up of joint operations within the meaning of article 24 of the Treaty. It suffices that the operational chiefs – for Luxembourg the Director General of the Grand-Ducal Police or his representative – of two ore more Parties involved come to an agreement. In any circumstance, contact should be taken first with the Operations Department of the Grand-Ducal Police which is the national contact point provided for by point 14.2 of the Implementing Agreement; it can be contacted as follows:

Police Grand-Ducale
Direction des Opérations
Adresse : 1, rue Marie et Pierre Curie
L-2957 LUXEMBOURG
Tel.: + 352 4997 – 2310
Fax : + 352 4997 – 2399
E-mail : dop@police.etat.lu

THE NETHERLANDS

Memberstates	Organisation	Central point of contact	Telephone number Fax number E-mail
AUSTRIA BELGIUM GERMANY FRANCE LUXEMBURG SPAIN	Korps Landelijke Politie Diensten (KLPD) Department for Conflict and Crisismanagement	Hoofdstraat 54 Postbus 100 3970 AC Driebergen	Tel:(0031)(0)343 535759 Fax(0031)(0)343 518180 E-Mail:ccb-klpd@klpd.politie.nl

SPAIN

National legislation and competencies in accordance to joint operations.

The Spanish legislation about joint operations is collected in the next legislation:

- Law 11/2003 about the joint investigations teams. This is the national law under the Frame Decision of 13 of June of 2002
- The development of article 40 "over border surveillance" we have the rules for this cases in the frame of the Schengen space. Here we have rules for the normal or urgent surveillance always under a judicial investigation, the type of criminal offences includes in this modality of cooperation, the Spanish competent authorities and the steps to do for using this surveillance and models of documents.
- Agreement with Portugal about joint and coordinate mobile controls of people.

We have no rules for other kinds of joint operations like joint patrols or similar.

In Spain we have many Treaties with different countries in order to improve the cooperation. We can highlight the next:

- **With Portugal:**
  - Agreement about readmission people in irregular situation signed the February 15, 1993 (Annexed)
  - Agreement about mobile controls signed the January 17, 1994. (Annexed)
  - Agreement about civil and penal matters signed the November 19, 1997 (Annexed)
  - Agreement about hot pursuit signed the November 30, 1998 (Annexed)
  - Agreement about border cooperation in police and custom matters signed the November 19, 2005 (Annexed)

- **With France**
  - Agreement about border cooperation in police and custom matters signed the July 7, 1998 (Annexed)

- Agreement about readmission people in irregular situation signed the November 26, 2002 (Annexed)
- Rules of organization and running of Cooperation Center (We have only in paper

NATIONAL CONTACT POINT

The national contact point in Spain is:

CENTRO PERMANENTE DE INFORMACIÓN Y COORDINACIÓN (CEPIC)

situated in:
Cabinete de Coordinación
Calle Amador de los Rios, 2

28010 MADRID- ESPAÑA

And the coordinates are: Phone numbers: + 34 915 371 883
+ 34 915 371 884
+ 34 915 372 056
+ 34 915 372 057
+ 34 915 372 058

FAX: + 34 913 191 228
+ 34 913 191 645
+ 34 913 197 389

MAIL: cepic@ses.mir.es

Model Request form
for joint operations on the basis of article 24 of the Treaty

Requesting Party:

- ❑ The Kingdom of Belgium, represented by the Directorate of the National Contact Point DGA/DAO

or

- ❑ The Federal Republic of Germany, represented by ....

or

- ❑ The Kingdom of Spain, represented by ....

or

- ❑ The French Republic, represented by ....

or

- ❑ The Grand Duchy of Luxembourg, represented by the Director General of the Grand-Ducal Police or his representative

or

- ❑ The Kingdom of the Netherlands, represented by ....

or

- ❑ The Republic of Austria, represented by ....

requests

- ❑ The Kingdom of Belgium, represented by the Directorate of the National Contact Point DGA/DAO

or

- ❑ The Federal Republic of Germany, represented by ....

or

- ❑ The Kingdom of Spain, represented by ....

or

- ❑ The French Republic, represented by ....

or

- ❑ The Grand Duchy of Luxembourg, represented by the Director General of the Grand-Ducal Police or his representative

or

- ❑ The Kingdom of the Netherlands, represented by ....

or

- ❑ The Republic of Austria, represented by ....

for the following:

❑ **Police intervention** by …… police officers, as detailed in the annex to the present request, in order to contribute to the maintenance of public order at:

…… (*place, zone; date*);

under the operational command of ……...……
(*name and function of the police officer*).

❑ **For agreement:**

❑ **The furnishing of means** for public order maintenance, as detailed in the annex to the present request.

These means will be deployed at ……..…… (*name of the place, name of the zone; date*);

under the operational command of ……...
(*name and function of the police officer*).

❑ **For agreement:**

❑ The dispatch of .....……..... police officers to accompany or operate the material means for that purpose.
❑ **For agreement :**

❑ **Other:**
❑ **For agreement:**

❑ **One border crossing**
❑ **Several border crossings during the following period:**
❑ **For agreement:**

Sovereign powers
❑ Requests to confer to the seconding state's officers the sovereign powers allowed by the Host State.
❑ **For agreement:**

❑ Requests to allow the Seconding State's officers to exercise their own sovereign powers in accordance with the Seconding State's law. If granted, the seconding state's officers will have the same sovereign powers as in their own country.
❑ **For agreement:**

Costs
❑ Each Contracting Party shall bear the costs incurred by its own authorities.
or
❑ Other proposition for the sharing out of the costs:

- **For agreement:**

…….……..… (*date*) ……..…… (*place*)

…… (*Signature*)

agreement

…….…… (*date*) ……..……. (*place*)

…… (*Signature*)

Annex D.2

Authorities to be notified without delay in case of a cross-border operation in the event of imminent danger, and

contact points for the reporting of modifications in the contact details listed in this Annex.

AUSTRIA

Border with	Name of Bundesland or ministry	Municipalities (border municipalities are in bold)	Telephone number Fax number E-mail
GERMANY	Landespolizeikommando Oberösterreich – Landesleitzentrale		Tel.: +43 (0) 59133 40-2222 Fax: +43 (0) 59133 40-1009 Mail: LPK-O@polizei.gv.at
	Landespolizeikommando Salzburg – Landesleitzentrale		Tel.: +43 (0) 59133 50-2222 Fax: +43 (0) 59133 50-1009 Mail: LPK-S@polizei.gv.at
	Landespolizeikommando Tirol – Landesleitzentrale		Tel.: +43 (0) 59133 70-2222 Fax: +43 (0) 59133 70-1009 Mail: LPK-T@polizei.gv.at

Border with	Name of Bundesland or ministry	Municipalities (border municipalities are in bold)	Telephone number Fax number E-mail
	Landespolizeikommando Vorarlberg – Landesleitzentrale		Tel.: +43 (0) 59133-80-2222 Fax: +43 (0) 59133-80-1009 Mail: LPK-V@polizei.gv.at
OTHER PARTYS	Federal Ministry of the Interior, Division II – General Directorate for Public Security, Operations and Crisis Coordination Centre		Phone: +431-53126-3200 or -3775 Fax: +431-53126-3120 e-mail: bmi-II-EKC-Permanenzdienst@bmi.gv.at

National contact points for the reporting of changes in the contact details in this Annex:

Federal Ministry of the Interior, General Directorate for Public Security,
Sub-Department II/2/a
Phone: +431-53126-3411
Fax: +431-53126-10-8638
e-mail: bmi-II-2-a@bmi.gv.at

BELGIUM

NB: In Belgium, it is necessary to contact both the national centre and the local zone concerned!

National Centre:

DAO
(Direction opérations concernant la police administrative)
Officier de permanence
Blok G, Fritz Toussaintstraat 47
Tél: 02 642 6380
Fax: 02 646 4940
Mail: dga-dao@skynet.be

Local police zone

Border with	Number (and name) of the policezone	Municipalities (border municipalities are in bold)	Telephone number
FRANCE	PZ 5461 WESTKUST	**DE PANNE** / KOKSIJDE / NIEUWPOORT	+ 32 (0) 58 53.30.00
	PZ 5459 SPOORKIN	**ALVERINGEM** /LO-RENINGE/**VEURNE**	+ 32 (0) 58 33.53.11
	PZ 5462 ARRO IEPER	**HEUVELLAND**/IEPER/LANGE MARK-POELKAPELLE/ MESEN/MOORSLEDE/ **POPERINGE**/ STADEN/VLETEREN/ **WERVIK**/ZONNEBEKE	+ 32 (0) 57 23.05.00
	PZ 5318	**COMINES-WARNETON**	+ 32 (0) 56 55.96.14
	PZ 5455 GRENSLEIE	LEDEGEM /**MENEN/ WEVELGEM**	+ 32 (0) 56 51.01.11
	PZ 5317	**MOUSCRON**	+ 32 (0) 56 86.07.00
	PZ 5320 DU VAL DE L'ESCAUT	CELLES/ **ESTAIMPUIS**/ MONT-DE-L'ENCLUS/PECQ	+ 32 (0) 69 53.29.30
	PZ 5316 DU TOURNAISIS	**TOURNAI/ANTOING/ RUMES/BRUNEHAUT**	+ 32 (0) 69 25.02.50
	PZ 5321	**BERNISSART/ PERUWELZ**	+ 32 (0) 69 77.20.57
	PZ 5329 DES HAUTS-PAYS	**DOUR/HENSIES/**HONNELLES/ **QUIEVRAIN**	+ 32 (0) 65 65.20.25
	PZ 5327 BORAINE	BOUSSU/COLFONTAINE/ **FRAMERIES**/ QUAREGNON/ SAINT-GHISLAIN	+ 32 (0) 65 61.00.20
	PZ 5324	MONS/QUEVY	+ 32 (0) 65 40.43.00
	PZ 5333 LERMES	**ERQUELINNES /** **ESTINNES**/LOBBES/MERBES	+ 32 (0) 71 59.76.30
	PZ 5334 BOTTE DU HAINAUT	**BEAUMONT/ CHIMAY**/ FROIDCHAPELLE/ **MOMIGNIES/SIVRY**	+ 32 (0) 60 41.40.70
	PZ 5311 3 VALLEES	**COUVIN /VIROINVAL**	+ 32 (0) 60 31.03.00
	PZ 5315 HERMETON ET HEURE	CERFONTAINE / DOISCHE / PHILIPPEVILLE	+ 32 (0) 71 66.02.11
	PZ 5312 HAUTE-MEUSE	ANHEE / DINANT/ **HASTIERE**/ ONHAYE/YVOIR	+ 32 (0) 82 21.42.98
	PZ 5310 HOUILLE-SEMOIS	**BEAURAING** /BIEVRE/ **GEDINNE/VRESSE-SUR-SEMOIS**	+ 32 (0) 61 58.70.26

Border with	Number (and name) of the policezone	Municipalities (border municipalities are in bold)	Telephone number
	PZ 5302 SEMOIS ET LESSE	BERTRIX/**BOUILLON**/ DAVERDISSE/ HERBEUMONT/ LIBIN/ PALISEUL / SAINT-HUBERT/ TELLIN / WELLIN	+ 32 (0) 61 46.60.07
	PZ 5299 DE GAUME	CHINY /ETALLE/ **FLORENVILLE/ MEIX-DEVANT VIRTON/ ROUVROY**/ TINTIGNY / **VIRTON**	+ 32 (0) 63 58.99.30
	PZ 5298 SUD-LUXEMBOURG	AUBANGE /**MESSANCY**/ **MUSSON**/SAINT-LEGER	+ 32 (0) 63 38.02.54
GERMANY	PZ 5292 WESER-GOHL	**EUPEN /KELMIS**/ LONTZEN/**RAEREN**	+ 32 (0) 87 59.55.00
	PZ 5290 STAVELOT-MALMEDY	LIERNEUX / MALMEDY / STAVELOT / STOUMONT / TROIS-PONTS /**WAIMES**	+ 32 (0) 80 28.18.00
	PZ 5291 EIFEL	AMEL /**BULLINGEN/ BUTGENBACH/ BURG-REULAND/ SANKT-VITH**	+ 32 (0) 80 28.14.10
LUXEM-BOURG	PZ 5298 SUD-LUXEMBOURG	**AUBANGE /MESSANCY/ MUSSON**/SAINT-LEGER	+ 32 (0) 63 38.02.54
	PZ 5297	**ARLON / ATTERT** / HABAY / **MARTELANGE**	+ 32 (0) 63 60.84.49
	PZ 5301 CENTRE ARDENNE	**BASTOGNE** / BERTOGNE / **FAUVILLERS**/LEGLISE/ LBRAMONT-CHEVIGNY/ NEUFCHATEAU/ SAINTE-ODE / VAUX-SUR-SURE	+ 32 (0) 61 24.12.11
	PZ 5300 FAMMENE-ARDENNE	DURBUY / EREZEE / **GOUVY** / HOTTON / **HOUFFALIZE** / LAROCHE-EN-ARDENNE/ MANHAY / MARCHE-EN-FAMENNE/NASSOGNE/ RENDEUX/TENNEVILLE/VIELSALM	+32 (0) 84 31.03.11
	PZ 5291 EIFEL	AMEL /**BULLINGEN/ BUTGENBACH/ BURG-REULAND/ SANKT-VITH**	+ 32 (0) 80 28.14.10

Border with	Number (and name) of the policezone	Municipalities (border municipalities are in bold)	Telephone number
NETHER-LANDS	PZ 5446	**DAMME / KNOKKE-HEIST**	+ 32 (0) 50 61.96.00
	PZ 5424	**MALDEGEM**	+ 32 (0) 50 72.71.60
	PZ 5417 MEETJESLAND CENTRUM	EEKLO / KAPRIJKE / **SINT-LAUREINS**	+ 32 (0) 9 376.46.46
	PZ 5421	**ASSENEDE** / EVERGEM	+ 32 (0) 9 257.00.10
	PZ 5416 REGIO PUYENBROECK	LOCHRISTI /**MOERBEKE / WACHTEBEKE / ZELZATE**	+ 32 (0) 9 355.74.40
	PZ 5431	**SINT-GILLIS-WAAS/STEKENE**	+ 32 (0) 3 470.27.30
	PZ 5430 BEVEREN	**BEVEREN**	+ 32 (0) 3 750.14.11
	PZ 5345	ANTWERPEN	+ 32 (0) 3 202.55.11
	PZ 5348 NOORD	**KAPELLEN / STABROEK**	+ 32 (0) 3 660.09.30
	PZ 5350 GRENS	**ESSEN** / KALMTHOUT / **WUUSTWEZEL**	+ 32 (0) 3 620.29.29
	PZ 5363 NOORDER-KEMPEN	**HOOGSTRATEN / MERKSPLAS /** RIJKEVORSEL	+ 32 (0) 3 340.88.00
	PZ 5364 REGIO TURNHOUT	**BAARLE-HERTOG** / BEERSE / KASTERLEE / LILLE / OUD-TURNHOUT / **TURNHOUT** / VORSELAAR	+ 32 (0) 14 40.85.50
	PZ 5367 KEMPEN NOORD-OOST	ARENDONK / **RAVELS** / RETIE	+ 32 (0) 14 40.40.60
	PZ 5368	BALEN / DESSEL / MOL	+ 32 (0) 14 33.07.00
	PZ 5371	LOMMEL	+ 32 (0) 11 54.43.60
	PZ 5372 HANO	**HAMONT-ACHEL** / NEERPELT / OVERPELT	+ 32 (0) 11 44.08.20
	PZ 5385 NOORD-OOST LIMBURG	BOCHOLT / BREE / KINROOI / MEEUWEN-GRUITRODE	+ 32 (0) 89 48.06.30
	PZ 5383 MAASLAND	DILSEN-STOKKEM / **MAASEIK**	+ 32 (0) 89 56.92.11
	PZ 5387	**MAASMECHELEN**	+ 32 (0) 89 76 97 00
	PZ 5386	**LANAKEN**	+32 (0) 89 71.22.23
	PZ 5381	BILZEN / HOESELT / RIEMST	+ 32 (0) 89 51 93 00
	PZ 5281 BASSE-MEUSE	**BASSENGE**/BLEGNY/DALHEM / JUPRELLE / OUPEYE / **VISE**	+ 32 (0) 4 374.88.00

Border with	Number (and name) of the policezone	Municipalities (border municipalities are in bold)	Telephone number
	PZ 5382	**VOEREN**	+ 32 (0) 4 381.10.11
	PZ 5288 PAYS DE HERVE	AUBEL/BAELEN/HERVE/LIMBOURG/OLNE / PLOMBIERES / THIMISTER-CLERMONT / WELKENRAEDT	+ 32 (0) 87 68.02.40

National contact points for the reporting of changes in the contact details listed in this Annex:

Police Fédérale belge
Direction de la politique en matière de coopération policière internationale (CGI)
Square Victoria Regina 1, 1210 Bruxelles
Tél.: + 32 2 223 98 50
Fax: + 32 2 223 98 82
E-mail: cg.cgi.srt@police.be

FRANCE

Border with	Organisation	Municipality	Telephone number Fax number E-mail
ITALY	CCPD	Vintimille	Tel: 04 92 41 15 70/71/72 Fax:04 92 41 15 74 E-mail: ccpd-vintimille.ddpaf-06@interieur.gouv.fr
	CCPD	Modane	Tel: 04 79 05 42 42 Fax:04 79 05 42 40 E-mail: ccpd-modane-73@wanadoo.fr
GERMANY	CCPD	Kehl	Tel: 0049.7851.8895-0 Fax: 03 90 23 13 69 E-mail: mailto:centro.lz@1.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or: fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)

Border with	Organisation	Municipality	Telephone number Fax number E-mail
SWITZERLAND	CCPD	Genève Cointrin	Tel: 04 50 28 47 00 Fax: 04 50 28 47 19 E-mail: ccpd-geneve.ddpaf-01@interieur.gouv.fr
SPAIN	CCPD	Hendaye	Tel: 05 59 20 93 60 Fax: 05 59 20 59 34 E-mail: ccpd-hendaye@interieur.gouv.fr
	CCPD	Le Perthus	Tel: 04 68 83 79 00 Fax: 04 68 83 79 10 Tel: 05 59 20 93 60 Fax: 05 59 20 59 34 E-mail: ccpd-hendaye@interieur.gouv.frccpd-sec.le-perthus-66@intermel.si.mi
	CCPD	Canfranc le Somport	Tel: 05 59 39 04 85 Fax: 05 59 36 18 15 E-mail: ccpd.canfranc@interieur.gouv.fr
	CCPD	Melles Pont du Roy	Tel: 05 61 94 68 40 Fax: 05 61 94 68 48 E-mail: ccpd.melles@interieur.gouv.fr
BELGIUM	CCPD	Tournai	Tel: 00 32 69 68 26 10 Fax: 00 32 69 68 26 21 E-mail: ccpd-tournai.dzaf-59@interieur.gouv.fr
LUXEMBOURG	CCPD	Luxembourg	Tel: 03 82 54 94 30 ou +352 26 124 300 Fax: 03 82 54 94 39 ou +352 26 124 199 E-mail: fr@bccp.etat.lu

National contact points for the reporting of changes in the contact details listed in this Annex:

Etat Major de la Direction Centrale de la Police aux Frontières
Centre d'information et de Commandement
Tel: + 33 1 40 07 66 95
Fax: + 33 1 42 65 15 85
E-mail: cic.dcpaf@interieur.gouv.fr

GERMANY

The officers crossing the border must notify the competent local police operations centre of the Länder police forces or the Federal Police.

Examples for border crossings:
"Ad hoc situations" when officers find suicidal or helpless persons, in case of traffic accidents, or when officers observe crimes with imminent danger for life and limb

Border with	Organisation	Municipality	Telephone number Fax number E-mail
All borders with the Prüm Partners (AT, FR, LU, BE, NL)	Local contactpoints of the police (Police of the Länder and Bundespolizei) In the event of a border crossing, the competent local Police Communications Centre of the Land police forces or of the Federal Police must be informed without delay	All municipalities at the borders with the Prüm partners	

National contact points for the reporting of changes in the contact details listed in this Annex and changes of contact details of the Länder police forces:

Bundeskriminalamt
65173 Wiesbaden
Tel: +49 611 55 13101
Fax: +49 611 55 12141;
E-mail: mail@bka.bund.de

LUXEMBOURG

Authority to be notified without delay in case of a cross-border operation in the event of imminent danger:

Police Grand-Ducale
Direction des Opérations
Centre d'Intervention National (CIN)
Adresse: 1, rue Marie et Pierre Curie
L-2957 LUXEMBOURG
Tel.: + 352 4997 – 2323
Fax: + 352 4997 – 2398
E-mail: cin@police.etat.lu

National contact point for the reporting of changes in the contact details listed in this Annex:

Police Grand-Ducale
Direction des Opérations et de la Prévention
Adresse: 1, rue Marie et Pierre Curie
L-2957 LUXEMBOURG
Tel.: + 352 4997 - 2310
Fax: + 352 4997 – 2399
E-mail: dop@police.etat.lu

THE NETHERLANDS

Border with	Organisation	Contact details	Telephone number Fax number E-mail
BELGIUM GERMANY	Korps Landelijke Politiediensten (KLPD) (Police) Bureau Conflict-en Crisisbeheersing	Hoofdstraat 54 Postbus 100 3970 AC Driebergen	Tel: (0031)(0)343536366 Fax: (0031)(0)343518180 E-mail: ccb.klpd@klpd.politie.nl

National contact points for the reporting of changes in the contact details listed in this Annex:

Korps Landelijke Politie Diensten (KLPD) Department for Conflict and Crisismanagement	Hoofdstraat 54 Postbus 100 3970 AC Driebergen	Tel: (0031)(0)343536366 Fax: (0031)(0)343518180 E-mail: ccb.klpd@klpd.politie.nl

SPAIN

The specified authorities to notify in the frame of the Treaty will be:

- The operational units mentioned in the Schengen agreement with France.
- Cooperation Centre between Spain and France situated in:

Border with	Organization	Municipality	Telephone number Fax number E-mail Timetable
FRANCE	CCPD	LE PERTHUS / LA JUNQUERA	Tel: 00 33 468 837913 Fax: 00 33 468 837920 E-mail: gi-smd-girona-ccpa@guardiacivil.org Timetable: Monday – Friday 08: 00 – 20:30
	CCPD	HENDAYA / IRÚN	Tel: 00 33 559 209360 / 00 34 696 909738 Fax: 00 33 559 205934 E-mail: ss-ccpa-hendaya@guardiacivil.org Timetable: 24 hours a day
	CCPD	SOMPORT (Huesca)	Tel: 00 34 974 373572 Fax: 00 34 974 373573 E-mail: hu-cmd-huesca-ccpasomport@guardiacivil.org Timetable: 24 hours a day
	CCPD	MELLES – PONT DU ROY	Tel: 00 33 561 892962 / 00 33 561 946840 Fax: 00 33 561 892639 E-mail: l-ccpa-melles@guardiacivil.org Timetable: Monday – Friday 08: 00 – 21: 00 Saturday – Sunday 09: 00 – 17: 00

PROVINCE HEADQUARTERS	ADDRESS	TELEPHONE NUMBER	FAX	EMAIL INTERNET
GUIPÚZCOA	C/ Barachategui, 59 20015 – San Sebastián	943-276611 (switchboard) 943-297918 Operational Service Center (COS)	943-292134	ss-cmd-sansebastian-cos@guardiacivil.org
NAVARRA	Avda. Galicia, 2 31003 – Pamplona	948-296850	948-296860	na-cmd-pamplona-cos@guardiacivil.org
HUESCA	Avda. Martínez Velasco, 83 22004 – Huesca	974-210074 974-210105 974-210252	974-211238	hu-cmd-huesca-cos@guardiacivil.org
LLEIDA	C/ Libertad, 3 25071 – Lleida	973-249008 (switchboard) 973-245633 (COS)	973-228422 973-246078	l-cmd-lleida-registro@guardiacivil.org
GIRONA	C/ Emilio Grahit, 52 17003 – Girona	972-208650 (switchboard) 972-484012 (COS) 972-426066	972-484000	gi-cmd-girona@guardiacivil.org

NACIONAL POLICE

REGION	UNIT	ADRESS	TELÉFONO	FAX
PAÍS VASCO	Headquarters of San Sebastián	C/ José Mª Salaverria, s/n	34.943.454800	34.943.457855
NAVARRA	Headquarters of Pamplona	C/ General Chinchilla, 3	34.948.299700	34.948.223326
ARAGÓN	Headquarters of Huesca	C/ Ricardo Arco, 7	34.974.245400	34.974.243320
CATALUÑA	Headquarters of Girona	C/ Sant Pau, 2	34.972.220025	34.972.201149
CATALUÑA	Headquarters of Lleida	C/ Paseo de Ronda, 54	34.973.264799	34.973.264799

National contact points for the reporting of changes in the contact details listed in this Annex:

CENTRO PERMANENTE DE INFORMACIÓN Y COORDINACIÓN (CEPIC)

situated in: Gabinete de Coordinación
Calle Amador de los Rios, 2
28010 MADRID – ESPAÑA

Phone numbers:	FAX:	E-MAIL:
+ 34 915 371 883	+ 34 913 191 228	cepic@ses.mir.es
+ 34 915 371 884	+ 34 913 191 645	
+ 34 915 372 056	+ 34 913 197 389	
+ 34 915 372 057		
+ 34 915 372 058		

Annex D.3

Particular arms, ammunition and equipment which are prohibited to be carried according to article 28 paragraph 1, 3rd phrase of the Treaty

Particular arms, ammunition and equipment which are prohibited to be used and the legal aspects according to article 28 paragraph 2 of the Treaty

Practical aspects of the use of arms, ammunition and equipment according to article 28 paragraph 5 of the Treaty

AUSTRIA

There are no prohibitions in Austria regarding article 28 paragraph 1, 3rd phrase and article 28 paragraph 2 of the Treaty.

LEGAL AND PRACTICAL CONDITIONS OF THE USE OF ARMS, AMMUNITION AND EQUIPMENT

Use of means of force and service weapons is regulated in the Federal Law of 27 March 1969 on the 'Use of Weapons by Officers of the Federal Police, Federal Gendarmery and police at community level ("Use of Weapons Act 1969)"; Federal Law Gazette No. 149/1969 (in the version of Fed.Law Gazette No. 146/1999).

2. § Officers of the Federal Police, Federal Gendarmery and police at community level are authorized to make use of their service weapons if the need arises when exercising their duty

1. in case of justified self-defence;
2. to overcome resistance against justified law enforcement intervention;
3. to enforce a lawful arrest;
4. to prevent the escape of a detained person;
5. to avert any form of danger.

3. § Service Weapons in the meaning of this Federal Law are

1. rubber truncheons, and other truncheons for police interventions,
2. tear gas and other irritants, which cause only a short-term health impairment
3. water canons,
4. firearms, as listed in category I., para. 1 and 2 of the Annex I to the State Treaty concerning the Restoration of an Independent And Democratic Austria, Federal Law Gazette No. 152/1955, which support the officers listed in § 2 to fulfil their duty as instructed by their superior authority or their service.

4. § Use of arms is admissible only, if lesser measures, such as the order to restore lawful condition, threat of use of firearms, pursuit of a fugitive, use of physical force, or other available lesser means, such as handcuffs or technical barriers, have proven unsuitable or ineffective.

5. § If different types of weapons are at disposal, only that weapon that appears least dangerous but still effective under the prevailing circumstances, may be used.

6. § (1) Use of weapons directed against human beings may only serve the purpose to make an individual incapable of resisting or fleeing. In cases as outlined in § 2, para. 2-to 5, the damage expected by use of weapons must not be disproportionate to the intended effect.
(2) Each weapon must be used with the greatest possible caution and care for human beings and property. Weapons may be directed against human beings only, if use of weapons against property would be ineffective.

Life-threatening Use of Weapons

7. § Use of weapons presenting a threat to life of human beings is admissible only:

1. in case of justified self-defence to defend a human being;
2. to suppress a riot or insurgence;

3. to enforce an arrest or prevent the escape of an individual strongly suspected of a crime than can only be committed deliberately and is liable to a prison term of more than one year, which in itself or in connection with the suspect's behaviour during arrest or escape shows there is a general security risk to the state, to himself or property;
4. to enforce arrest or prevent the escape of a mentally deranged person who poses a general security risk to himself or property.

8. § (1) A distinct warning must be given immediately before life-threatening use of weapons against human beings. If there is a crowd, the warning must be repeated. firing a warning shot also counts as warning.
(2) Life-threatening use of weapons is admissible only, if there is no risk for innocent by-standers, unless it appears inevitable in order to prevent a crowd from violent actions, posing a direct or indirect security risk to individuals.
(3) In case of justified self-defence, the provisions of paragraphs 1 and 2 do not apply.

Use of other means than service weapons and of means having the effect of a weapon

9. § If a suitable service weapon is not available, also other weapons, or means having the effect of a weapon, may be used by applying the provisions of the federal law mutatis mutandis.

BELGIUM

Particular arms, ammunition and equipment which are prohibited to be carried:

For the cross-border operations provided in article 25: no prohibitions in Belgium
For the other forms of cross-border operations: police officers are allowed to carry the arms, ammunition and equipment that they are allowed to use in Belgium.

Particular arms, ammunition and equipment which are prohibited to be used:

Belgium permits the use of the arms, ammunition and equipment listed in Annex 2 of the Treaty. The Seconding State's officers operating on Belgian territory should take into account the following principles:

- Belgium does not permit the use of firearms with a calibre that exceeds 9 mm;
- Belgium does not permit the use of firearms in fully automatic mode;
- Belgium does not permit the use of any type of handcuffs that can injure the apprehended person;
- Belgium permits the use of pepperspray but does not permit the use of tear gas Chloroacetophone (CN);
- Belgium does not permit the use of electric truncheons but permits the use of ordinary truncheons;
- Belgium does not permit the use of TASER).

Legal and practical conditions of the use of authorised arms, ammunition and equipment (art. 28).

1. Self defence

Art 38 Law on the police function

Without prejudice to Art 37, police officers are only allowed to use firearms against people if they are acting in self-defence.

Art 416 of the penal code

Committing homicide or assault in legitimate self-defence may not be regarded as a crime or as an offence.

Explanation of Art 416 of the penal code.

- Self-defence applies to everybody, not only police officers.
- Acts of self-defence may occur against all kinds of violence, not only against firearms.
- In order to be regarded as self-defence, any situation has to fulfil the following requirements:
  - **The assault has begun or is about to begin.**
    The victim must not necessarily be in danger of life. Running a real and grave risk of being injured or wounded is sufficient.

    The assault is illegal.
    There is no self-defence against legal and justified assault. For instance, it is not allowed to use violence against legal police actions.

  - **The assault must be committed against people.**
    In art 416 of the penal code, insults are not regarded as assaults against people.

  - **Self-defence must be necessary and proportional.**
    If self-defence goes beyond the necessary limits, if the defence is more violent than the assault, it becomes an assault itself. As far as proportionality is concerned, the consequences of the use of a weapon must always be taken into account. For instance, hitting someone's head with a claw may be as lethal as a gunshot. If you are not in a position to defend yourself in another way and if you are in danger of life, the use of a firearm is then justified.

  - **Defence must occur at the same time as the assault.**
    Self-defence must not be a vengeance and, consequently, occur when the assault is over.

Art 417 of the penal code

Besides the provision of Art 416 of the penal code, two other cases can be regarded as self-defence. They are explained in Art 417 of the penal code:

Both following cases may be regarded as legitimate self-defence:

If homicide or assault has been committed while repelling, at night, someone climbing a fence or a wall or breaking into an occupied house or flat or their outbuildings, unless a constable considers that the person who climbed or broke in did not have the intention of making a murder attempt, either before his/her acts or as a consequence of the resistance of the occupants.

If the fact occurred while defending oneself against authors of theft or looting with assault and battery.

Giving a warning.

In accordance with article 37 of the law on the police function, any resort to force must be preceded by a warning, unless this warning makes it ineffective.

The important point here is that we can use a firearm in a preventive and repressive way. The preventive use of the firearm includes intimidating the opponent. In this case, no shot is fired. The firearm is only used preventively.

The repressive use can be subdivided into three parts:

a. Intimidation shot. An intimidation shot is fired when the policeman is not directly threatened. He fires in the air to intimidate the opponent.
b. Warning shot. A warning shot is fired when the policeman is threatened. In this case, he does not fire at the opponent.
c. Shot at people, animals or objects. This may occur in self-defence or in the other cases provided for in the law on the police function.

In brief, we can state that the use of force is preceded by a warning. This warning may be a verbal order or a warning shot, unless this warning makes the resort to force ineffective or in case of self-defence.

2. The use of force

In Belgium, firearms and ammunition can only be used in case of legitimate defence. In accordance with Art 28, paragraph 2 of the Treaty, however, the Belgian officer in charge of the operation may, in individual cases, give permission to use the other authorised arms and equipment for purposes going beyond the legitimate defence. However, the use of these arms and equipment will always have to be in accordance with the Belgian national law.

Art 37: Law on the police function

In the exercise of his duties, any police officer may resort to force, on the following conditions:

1. He has to take all the risks of this resort to force into account;
2. He has to pursue a legitimate objective (that could not be reached otherwise);
3. The resort to force must be sensible and proportional to the pursued objective;
4. The resort to force must be preceded by a warning (unless this warning makes it ineffective).

Explanation of Art 37.

The first three conditions of Art 37 may come down to only one word:

1. Opportunity: The policeman must take the risks of the use of force into account, from both physical and material points of view.

E.g.: During a control, a policeman fires at the tyres of a leaving vehicle but the bullet misses the target and hits an innocent passenger.

2. Legality: The use of force and coercion is only allowed in the cases and on the conditions provided for in the law.

E.g.: During an identity check, the person being controlled wants to punch your colleague. You react immediately by getting the person in a self-defence hold.

3. Proportionality: If the use of force and coercion is necessary, the less violent and most appropriate solution will then be chosen.

E.g.: During a fight in a pub, a drunken person takes a bottle and makes as if to hit another person with it. The drunken person does not react to your verbal warnings. As this person is drunk and armed, you take your truncheon and try to overcome him.

In short, one always has to consider three questions before resorting to force.

1. Is it legal?
2. Aren't there any less violent and dangerous means?
3. Are the means proportional to the goal to be achieved?

FRANCE

France does not foresee any restrictions with respect to carrying service weapons, means of force and other equipment provided they have been handed out by the police administration of the Prüm partners. While enforcing article 25, the use of weapons and firearms shall be restricted to self defense situations and only handguns (revolvers and pistol guns) tear gas and truncheons, as long as they have been handed out by the police administration, will be allowed.

Legal and practical conditions of the use of arms, ammunition and equipment

Specific conditions under which self defense is admitted.

Requirements for self defense in French criminal law are stated in the articles 122-5 and 122-6 of the penal code. While the first one explains the general conditions of self defense, the second describes two particular situations which reacting to will be considered as necessitated by self defense.

Firstly, self defense is a reaction to protect a victim from an assault and article 122-5 specifies the details of its two components that are the attack and the counterattack.

The attack has first to be perpetrated against a person, policeman or not. It has then to be unjustified which obviously is not the case when rebelling against enforcement of the law by the police. It has last to be real and current which on the one hand, means that using weapons or firearms to react to a threat cannot be justified by the needs of self defense and on the other hand, means that using weapons and firearm after the attack is finished would be considered as retaliation instead of self defense.

For the same reason that just explained the counterattack must be immediate while the assault as not to be considered as retaliation. It has then to be necessary which means only it could stop the attack. Finally it has to be commensurate with the attack.

Secondly, self defense is a reaction in order to interrupt a crime or an offense against possessions while it is being perpetrated. In such a situation article 122-5 states that self defense act has to be strictly necessary and commensurate with the infringement seriousness as long as it is not a murder.

Article 122-5 states that there is no penal liability for a person acting for self defense needs.

The concerns of article 122-6 are about two particular situations in which the use of weapon or firearm by a policeman would be presumed as necessitated by self defense.
The first one is related to a case where policeman act to repel out of a lived in property the perpetrator(s) of a burglary committed by means of a trick or violence.
The second one is related to a situation where policeman act to defend himself against the perpetrators of a rubbery or of a looting committed with violence.
The presumption stated in article 122-6 is not irrefragable and does not exempt the person acting for self defense from having respect for particularities specified in article 122-5 such as reacting to a serious, real and current danger.

Particular situation stated in article 73 of criminal procedure code.

This article states that any citizen who sees a crime or an offense while it is being committed can arrest its perpetrator in order to present him to the local police officer. So for a foreign police officer crossing the French boarder as to enforce article 25 of the Prüm treaty can arrest an offender or a criminal provided that the arrest is done while the infringement is being committed.

GERMANY

Arms, ammunition and equipment prohibited from being carried during cross border operations (art 28)
For all kinds of operations: no prohibitions

Legal and practical conditions of the use of authorized arms, ammunition and equipment:

For Germany are relevant the "Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (BGBl. I 1961, 165; zuletzt geändert durch Art. 28 V vom 31.10.2006) and the equivalent laws of the federal Länder.

LUXEMBOURG

Particular arms, ammunition and equipment which are prohibited to be carried:

For the joint operations and the cross-border operations provided for by the articles 24 and 25 of the Treaty, there are in principle no prohibitions; the police officers of the other Parties are allowed to carry the arms, ammunition and equipment which are part of their individual or collective regular equipment.

For the joint operations provided for by article 24 of the Treaty, the mission statement foreseen in point 14.1 of the Implementing Agreement may specify some equipment which may not be carried for a determined operation.

Particular arms, ammunition and equipment which are prohibited to be used:

Luxembourg permits the use of the arms, ammunition and equipment listed in Annex 2 of the Treaty. The Seconding State's officers operating on Luxembourg territory should take into account the following principles:

Legal and practical conditions of the use of authorised arms, ammunition and equipment:

1. Self defence:

Luxembourg police officers – and hence also the police officers of other Parties operating on the Luxembourg territory within the framework of the Treaty – are in principle submitted to the general rules of self defence on the basis of articles 416 and 417 of the Penal Code, providing that homicide or assault committed in legitimate self defence may not be regarded as a crime or as an offence. Self defence may be practiced not only against firearms, but against all kinds of physical violence.

In order to be accepted as self defence, the following conditions have to be fulfilled:

1) *The assault must be illegal.*
There is no self defence against legal and justified assault. For instance, it is not allowed to use violence against legal police actions.

2) *Self defence must occur at the same time as the assault.*
Self-defence must begin at the latest when the assault is still ongoing; any act of defence started after the assault has ceased is not considered as self defence. Hence, all acts like physical violence against an offender who is fleeing or vengeance is outside the scope of self defence.

3) *Self-defence must be necessary and proportional.*
Acts going beyond the necessary limits to avoid an assault causing the risk of death or physical injuries may become by itself an assault. The consequences of the use of a weapon must always be taken into account. For instance, hitting someone's head with a claw may be as lethal as a gunshot. If you are not in a position to defend yourself in another way and if you are in danger of life, the use of a firearm is then justified.
As far as proportionality is concerned, it has to be stressed that an act of defence being more violent than the assault may also become an assault itself. On the other hand, the victim must not necessarily be in danger of life; running a real and grave risk of being injured or wounded is sufficient.

4) *The assault must consist in physical violence.*
All kinds of insults or verbal attacks are not regarded as assault justifying self defence.

5) *Self defence has, in principle, to be used in case of an assault against human beings.*
The fact of defending a third person against an assault is also considered as self defence if all the other conditions are fulfilled. Moreover, self defence in order to protect goods is in theory accepted but the condition of proportionality is in that case difficult to fulfil. Injuring or even killing a person as defence against a theft for example is in principle never considered as self defence.

Beside the situation of self defence as such, there are two cases which may be regarded as legitimate self-defence:

b) If homicide or assault has been committed while repelling, at night, someone climbing a fence or a wall or breaking into an occupied house or flat or their outbuildings, unless the person who climbed or broke in did not have the intention of making a murder attempt, either before his acts or as a consequence of the resistance of the occupants.
c) If the fact occurred while defending oneself against authors of theft or looting with assault and battery.

2. The use of police force, independently from self defence as such:

Beside the rules related to self defence, police officers are allowed in Luxembourg to make use of arms, firearms and other means of constraint according to the conditions provided for by the law of 28th July 1973 concerning the use of weapons and other means of constraint by the members of the public force in the fight against criminality.

These provisions may me summarised as follows:

Police officers on duty may, if it is absolutely necessary, use firearms and other arms:
1) if they are attacked, with or without arms;
2) if they are about to help other another person whose life, physical integrity or goods are considerably endangered;
3) if it is the only mean to defend, against an armed or unarmed attack, persons, posts, buildings or other installations which they are to protect;
4) if persons, who have been summoned twice to stop by the call "stop, police !", don't stop or if they cannot be stopped otherwise; however, in that second case, the use of weapons is only justified if there are reasonable grounds to believe:
   a) that these persons, identified or not, have committed a crime;
   b) that these persons are researched on the basis of an arrest warrant for crime;
   c) that these persons are fleeing prisoners or indicted persons.

Police officers may also use their weapons under the above mentioned conditions:
1) against persons who are fleeing after an attack and who don't after having been summoned to stop;
2) to push back person trying to take possession of prisoners, seized or confiscated goods and evidence after having been summoned to desist;
3) if there are no other means to stop a vehicles, boat or aircraft;
4) to prevent the imminent commission of a crime or offence.

The above mentioned use of weapons is also allowed to protect transports of money and other similar values.

The detailed provisions of the abovementioned law of 28th July 1973 are listed hereunder in excerpts in French and German.

Loi du 28 juillet 1973 réglant l´usage des armes et autres moyens de contrainte par les membres de la force publique dans la lutte contre la criminalité.

(Extrait)

Art. 1er. Dans l'exercice de leurs fonctions, les membres de la police grand-ducale peuvent, en cas de nécessité absolue, faire usage des armes blanches ou des armes à feu dans les cas suivants:
5) lorsque des violences ou voies de fait sont exercées contre eux, ou lorsqu'ils sont attaqués même sans armes ou qu'ils sont menacés par des individus armés;
6) lorsqu'ils sont appelés à prêter assistance à des personnes attaquées et dont la vie, l'intégrité physique ou les biens sont exposés à un danger considérable et présent;
7) lorsqu'ils ne peuvent défendre autrement, contre une attaque armée ou non, le terrain qu'ils occupent, les postes, édifices et installations qui leur sont confiés ou qui sont sous leur garde, ou encore les personnes à eux confiées ou sous leur escorte;
8) lorsque les personnes sommées de s'arrêter par deux appels, faits à haute voix, de «Halte, police !», cherchent à se soustraire à leurs investigations ou à l'arrestation, et ne peuvent être contraintes de s'arrêter que par l´usage des armes; toutefois, dans ce cas l'usage des armes n'est justifié que s'il y a des présomptions graves:

a) que les individus en question, identifiés ou non, ont commis un crime, et notamment s'ils sont poursuivis par la clameur publique;

b) ou que ces individus sont des personnes recherchées ou dont l'arrestation est ordonnée par un mandat de justice, pour crime;

c) ou que ces individus sont des prisonniers, détenus ou condamnés évadés, et qui sont recherchés, inculpés ou condamnés du chef de crime.

Art. 2. Les membres de la police grand-ducale peuvent encore faire usage de leurs armes, dans les conditions spécifiées à l'article 1er:

1) contre les personnes qui, sans obéir à l'ordre de s´arrêter, fuient après les avoir attaqués à main armée, et contre les conducteurs de véhicules pourvus de moteurs mécaniques qui fuient après avoir manœuvré pour mettre leur vie en péril;
2) pour repousser ceux qui, malgré la sommation de se désister ou de s'éloigner, tentent de leur enlever leurs prisonniers, leurs armes ou les objets saisis en vue de la confiscation ou à titre de pièces de conviction;
3) lorsqu'ils ne peuvent immobilier autrement les véhicules, embarcations, aéronefs ou autres moyens servant au transport d´auteurs présumés d´un crime dont les conducteurs n'obtempèrent pas à l'ordre ou au signal d'arrêt, sans préjudice de ce qui est porté à l'article 8 ci-après; lorsqu'un barrage dressé dans le cadre de la recherche des malfaiteurs a été forcé par un véhicule, et s'il appert des circonstances qu'il l'a été en connaissance de cause, le feu peut être ouvert sans sommation;
4) pour empêcher la commission imminente d'une infraction ou la continuation de cette infraction, si, d´après les circonstances, celle-ci constitue soit un crime, soit un délit commis à l'aide d´armes ou d´explosifs.

Art. 3. Dans les cas où il y a rébellion de la part des prisonniers ou tentative d'évasion, et s'il n'y a pas d'autres moyens de contenir ou de contraindre les révoltés ou les fuyards, le chef de l'escorte leur enjoint de rentrer dans l´ordre par les mots: «Halte ou je fais feu». Si cette injonction n'est pas suivie, l'usage des armes est autorisé.

Si les prisonniers cherchent à s'emparer des armes des membres de l'escorte, ou fuient après avoir blessé un membre de celle-ci, les armes peuvent être employées à l'instant et sans sommation préalable.

Art. 4. (…)

Art. 5. (…)

Art. 6. En cas de transport de fonds ou valeurs publics ou privés, les membres de la force publique qui forment l'escorte, en exécution des ordres reçus, peuvent ouvrir le feu dès qu'une attaque contre le convoi se manifeste par des actes extérieurs qui en forment un commencement d´exécution même s'ils ne sont pas personnellement en état de légitime défense. Si les assaillants fuient après s'être emparés de tout ou partie des valeurs convoyées, le feu peut être ouvert sur eux et leurs véhicules sans sommation.

Art. 7. Les prescriptions des articles 1 à 4 et 6 s'appliquent également à l'usage des gaz lacrymogènes et du matériel d´arrosage.

Art. 8. Dans le cadre de leurs opérations de contrôle et de recherche, les fonctionnaires visés à l'article 1er opérant d'office ou sur les ordres de leurs supérieurs hiérarchiques ou sur la réquisition de l'autorité judiciaire peuvent immobilier les véhicules de toute nature au moyen de câbles, herses, hérissons, barrières, filets et autres engins analogues.

Art. 9. (…)

Art. 10. Lorsque, dans l´exercice de ses fonctions, un membre de la force publique a reçu de son supérieur l'ordre d'employer les armes ou un moyen de contrainte quelconque, cet ordre est à exécuter, à moins qu'il ne concerne pas l'exécution des fonctions.
L'ordre ne doit pas être exécuté, si son exécution constituait un crime ou un délit.
Si, dans ce cas, l'ordre est néanmoins exécuté, l'agent d'exécution n'est responsable que s'il a connu ou pu connaître d'après les circonstances qu'il s'agissait manifestement d'un crime ou délit.
L'agent d'exécution doit, si les circonstances le lui permettent, faire valoir à l'égard de l'auteur de l'ordre ses objections en ce qui concerne la légalité de l'ordre reçu.

Art. 11. La présente loi ne déroge ni aux dispositions légales concernant le droit de légitime défense, ni aux dispositions de lois particulières qui autorisent, dans certains cas et au profit de certains agents et fonctionnaires, l'emploi de moyens de contrainte ou l'usage des armes dans une mesure plus étendue.
(…)

Gesetz vom 28. Juli 1973 über die Reglementierung des Gebrauchs von Waffen und anderen Zwangsmittel durch die Mitglieder der öffentlichen Macht im Kampfe gegen die Kriminalität. (Auszug)

Art. 1. Die Mitglieder der grossherzoglichen Polizei können, in Ausübung ihrer Pflicht und im Falle absoluter Notwendigkeit, in folgenden Fällen Gebrauch von Blank- oder Schusswaffen machen:

1) wenn Gewalttätigkeiten oder Tätlichkeiten gegen sie ausgeübt werden, oder wenn sie angegriffen werden, selbst ohne Waffen, oder wenn sie von bewaffneten Individuen bedroht werden;
2) wenn sie angegriffenen Personen Beistand leisten sollen, deren Leben, physische Unversehrtheit oder Eigentum einer beträchtlichen und gegenwärtigen Gefahr ausgesetzt sind;
3) wenn sie das von ihnen besetzte Gelände, die ihnen anvertrauten oder unter ihrer Bewachung stehenden Posten, Gebäude und Einrichtungen, oder aber die ihnen anvertrauten oder von ihnen eskortierten Personen nicht anders gegen einen bewaffneten oder nicht bewaffneten Angriff verteidigen können;

4) wenn die durch zwei, mit lauter Stimme gemachten Aufforderungen « Halt, Polizei ! » zum Stehen bleiben aufgeforderten Personen versuchen, sich ihrer Untersuchung oder Verhaftung zu entziehen, und nicht anders als durch den Gebrauch von Waffen zum Stehen bleiben gezwungen werden können; jedoch ist der Waffengebrauch in diesem Falle nur gerechtfertigt, wenn ernsthafte Vermutungen vorhanden sind:
   a) dass die betreffenden Individuen, ob identifiziert oder nicht, ein Verbrechen begangen haben, und besonders wenn sie vom öffentlichen Nachruf verfolgt werden;
   b) oder dass diese Individuen wegen eines Verbrechens gesucht werden, oder ihre Verhaftung wegen eines Verbrechens gerichtlich angeordnet worden ist;
   c) oder dass es sich bei diesen Individuen um entflohene Gefangene, Inhaftierte oder Verurteilte handelt, die wegen eines Verbrechens gesucht, beschuldigt oder verurteilt sind.

Art. 2. Die Mitglieder der grossherzoglichen der Polizei können, gemäss den in Artikel 1 bezeichneten Bedingungen, auch ihre Waffen gebrauchen:

1) Gegen Personen welche dem Befehl Stehen zu keine Folge leisten, die Flucht ergreifen nachdem sie die Beamten mit bewaffneter Hand angegriffen haben, sowie gegen die Fahrer von Kraftfahrzeugen die flüchtig werden, nachdem sie manövriert haben um das Leben der Beamten in Gefahr zu bringen;
2) Um diejenigen abzuwehren die, trotz Aufforderung von ihrem Vorhaben zu lassen oder sich zu entfernen, versuchen ihnen ihre Gefangenen, ihre Waffen oder die zwecks Einziehung oder als Beweisstücke beschlagnahmten Gegenstände zu entreissen;
3) Wenn sie nicht anders Fahrzeuge, Boote, Luftfahrzeuge oder sonstige Mittel zum Stillstand bringen können, die zur Beförderung der mutmaßlichen Urheber eines Verbrechens diesen und deren Fahrer dem Befehl oder dem Signal zum Halten keine Folge leisten, dies unbeschadet der Bestimmungen des nachstehend angeführten Artikels 8; das Feuer kann ohne Aufforderung eröffnet werden, wenn eine im Rahmen einer Fahndung errichtete Verkehrssperre von einem Kraftfahrzeug durchbrochen wurde, und sich aus dem Umständen ergibt, dass dies in voller Kenntnis der Sachlage geschehen ist;
4) Um das unmittelbar bevorstehende Begehen einer Zuwiderhandlung, oder um die Fortsetzung dieser Zuwiderhandlung zu verhindern wenn, den Umständen gemäss, es sich dabei um ein Verbrechen oder um ein mittels Waffen oder Sprengstoffen begangenes Vergehen handelt.

Art. 3. Wenn im Falle einer Rebellion oder eines Fluchtversuches von Gefangenen es nicht anders möglich ist die Rebellierenden oder Flüchtenden zurückzuhalten oder zu bezwingen, so befiehlt ihnen der befehlshabende Beamte die Ordnung wiederherzustellen mit den Worten « Halt oder ich schieße ! ». Wird diesem Befehl keine Folge geleistet, so ist der Gebrauch von Waffen erlaubt.

Die Waffen können sofort und ohne vorherige Aufforderung gebraucht werden wenn die Gefangenen versuchen sich der Waffen der Beamten zu bemächtigen oder flüchtig werden, nachdem sie einen dieser Beamten verwundet haben.

Art. 4. (…)

Art. 5. (…)

Art. 6. Sobald im Falle eines Geldtransportes oder eines Transportes von öffentlichen oder privaten Werten sich ein Angriff auf den Transport durch äußere Handlungen bemerkbar macht, die einen Anfang der Ausführung bilden, können die in Ausführung der erhaltenen Befehle die Eskorte bildenden Beamten das Feuer eröffnen, selbst wenn sie sich persönlich nicht im Zustand der rechtmäßigen Verteidigung befinden. Gehen die Angreifer flüchtig, nachdem sie sich der eskortierten Werte ganz oder teilweise bemächtigt haben, kann das Feuer auf sie oder ihre Fahrzeuge ohne Aufforderung eröffnet werden.

Art. 7. Die Bestimmungen der Artikel 1 bis 4 und 6 sind ebenfalls anwendbar auf den Gebrauch von Tränengas und Wasserwerfern.

Art. 8. Im Rahmen ihrer Kontroll- und Fahndungsoperationen können die in Artikel 1 erwähnten Beamten, ob von Amts wegen oder auf Befehl ihrer Vorgesetzten, oder auf Anordnung der Gerichtsbehörden, Fahrzeuge aller Art mittels Kabeln, Sturmeggen, Eisenspitzen, Sperren, Netzen und ähnlichen Vorrichtungen zum Stillstand bringen.

Art. 9. (…)

Art. 10. Wenn, in Ausübung seiner Dienstpflicht, ein Mitglied der öffentlichen Macht von seinem Vorgesetzten den Befehl erhalten hat, die Waffen oder irgendein Zwangsmittel zu gebrauchen, so ist dieser Befehl auszuführen, es sei denn er betreffe nicht die Ausübung der Dienstpflicht.

Der Befehl darf nicht ausgeführt werden, wenn seine Ausführung ein Verbrechen oder ein Vergehen darstellen würde.

Wenn in diesem Falle der Befehl trotzdem ausgeführt wird, so ist der ausführende Beamte nur dann verantwortlich, wenn er gewusst hat, oder den Umständen nach wissen konnte, dass es sich offensichtlich um ein Verbrechen oder Vergehen handelte.

Der ausführende Beamte muss, wenn die Umstände es ihm erlauben, dem Urheber des Befehls gegenüber seine Einwendungen bezüglich der Gesetzmäßigkeit des erhaltenen Befehls geltend machen.

Art. 11. Gegenwärtiges Gesetz beeinträchtigt weder die gesetzlichen Bestimmungen betreffend das Recht zur Notwehr, noch die Bestimmungen besonderer Gesetze, welche in gewissen Fällen Beamten die Anwendung von Zwangsmitteln oder den Gebrauch von Waffen in weiterem Sinne erlauben.
(…)

3. Particular situation provided for in article 43 of the Criminal Procedure Code:

According to this article, any person who sees another person in the act of committing a crime or an offence punished with deprivation of liberty is authorized to apprehend the offender and to conduct him before the next judicial police officer.
As a foreign police officer, being on the territory of Luxembourg within the framework of articles 24 and 25 of the Treaty, has the same rights as any person, he or she may act on behalf of this article, if not otherwise decided by a Luxembourg police officer according to article 24 paragraph 3 or article 25 paragraph 3, last phrase, of the Treaty.

THE NETHERLANDS

The Netherlands does not foresee any restrictions with respect to carrying service weapons, means for force, and other equipment (provided they have been handed out by the employer).

Article 28 paragraph 2 of the Treaty forms an exception to the following legislation. The arms, ammunition and equipment mentioned in Annex 2 (for the Netherlands: firearms, pepper spray and tear gas) may only be used in the legitimate defence of the officer himself or another (self-defence article 41 of the Penal Code). On the basis of the same provision the superior may determine otherwise in individual cases.

Police Act 1993

Article 8

-1. A police officer who is appointed to carry out a police task is authorised to use force in the lawful performance of his job, if the relevant goal justifies such, taking account of the risks inherent in the use of force and such goal cannot be achieved in a different manner. If possible the use of force shall be preceded by a warning.

-2. A police officer who has been appointed to carry out police duties has access to every location, insofar as such is reasonably necessary to provide assistance to those who require such.

-3. A police officer who has been appointed to carry out a police task is authorised to search the clothing of persons in the exercising of a power granted to him by law or when carrying out an action to perform the police task, if facts or circumstances show that there is an immediate risk for their life or safety, or the life or safety of the officer himself or of third parties and this search is necessary to deflect that risk.

-4. The district attorney or the assistant district attorney before whom detainees or suspects or convicts legally deprived of their freedom are brought, has the power to determine that their person will be

searched, if facts or circumstances show that there is a risk to their life or safety or the life or safety of the officer himself and this search is necessary to deflect that risk.

-5. The exercising of the powers referred to in paragraphs 1 through 4 must be reasonable and proportionate to the intended goal.

-6. Paragraphs 1 through 5 also apply to a member of the military police, if he acts in the lawful performance of his duties, and to members of any other part of the armed forces who assist the police on the basis of this Act.

-7. Our Minister of Justice can stipulate that the special investigating officers referred to in article 142, paragraph 1 of the Code of Criminal Procedure can exercise the powers described in paragraphs 1 and 3 insofar as designated by him either in person or per category or unit. In such case an official instruction shall be established for them in accordance with article 9.

Article 9

-1. By order in council on the proposal of Our Ministers of Justice and of the Interior and Kingdom Relations, in conjunction with Our Minister of Defence insofar as the military police is concerned, an official instruction shall be established for the police and for the military police.

-2. If a member of any other part of the armed forces acts in the performance of his tasks described in articles 59 and 60, the official instruction applies.

-3. The official instruction shall lay down rules for the implementation of articles 7 and 8.

-4. By or pursuant to an order in council, rules shall be established by ministerial regulation regarding measures which can be applied to persons lawfully deprived of their liberty with an eye on their detention, insofar as this is necessary in the interest of their safety or the safety of others. The order in council shall be established following a proposal of Our Ministers of Justice, and of the Interior and Kingdom Relations, in conjunction with Our Minister of Defence insofar as the military police is concerned.

-5. Paragraph 4 applies mutatis mutandis to persons who have been placed in the custody of the police or the military police in connection with assistance being given to them.

-6. Officers whom Our Minister of Justice has appointed to transport persons lawfully deprived of their freedom can exercise the powers referred to in article 8, paragraphs 1 and 3, or take the measures referred to in paragraph 4 insofar as this is necessary to prevent the person being transported from escaping custody. The first full sentence applies insofar as the persons lawfully deprived of their freedom are in the custody of the police or the military police.

Decree of 8 April 1994, establishing rules relating to a new Official Instruction for the police, the military police and special investigating officers and the measures which can be taken in respect of people who have been lawfully deprived of their liberty

(Official Instruction for the police, the military police and special investigating officers [Version effective as of: 20-09-2006])

History: Staatsblad 1994, 825; Staatsblad 1997, 764; Staatsblad 1998, 340; Staatsblad 1999, 197; Staatsblad 2001, 387; Staatsblad 2002, 174; Staatsblad 2004, 218; Staatsblad 2005, 110; Staatsblad 2006, 407

We Beatrix, by the grace of God, Queen of the Netherlands, Princess of Orange-Nassau, etc., etc., etc.

On the proposal of Our Ministers of Justice and of the Interior of 8 December 1993, Public Law Legislation Staff Department, no. 415284/93/6 and no. EA 93/U 3630, made in conjunction with Our Minister of Defence, no. CWW 85/008;

In view of article 9 of the Police Act 1993;

Having heard the Council of State (advice of 28 March 1994, no. W.O. 3.93.0838);

In view of the additional report of Our Minister of Justice which was also made on behalf of Our Minister of the Interior of 7 April 1994, Public Law Legislation Staff Department, no. 433019/94/6, no. EA 94/U1149, published in accordance with Our Minister of Defence;

Have approved and understood:

CHAPTER 1. General

Article 1

1. In this Decree officer is understood to mean:

a. a police officer as referred to in article 3, paragraph 1 under *a* and *c*, and paragraph 2 of the Police Act 1993;

b. a police officer as referred to in article 3, paragraph 1, under *b*, of the Police Act 1993 insofar as it relates to articles 1 and 2, chapter 5; In chapter 6 of this Decree officer also means a police officer as referred to in article 3, paragraph 1, under *b*, of the Police Act 1993, or another person, insofar as said police officer or said person is also a special investigating officer and has been charged by the police commissioner with taking care of detainees.

c. a person who is appointed as trainee for the term of his training;

d. members of the military police in the performance of police duties as referred to in article 6, paragraph 1 of the Police Act 1993;

e. members of the armed forces as referred to in article 59, paragraph 1 and article 60 of the Police Act 1993.

2. In this Decree the following terms have the following meaning:

a. an officer who under the heading of his duties or pursuant to an order or instruction is charged with or has command of the performance of the duties;

b. if on the basis of the provisions under *a*, no superior can be designated, the police officer who has a higher rank or, in the event of equal ranks, the person with the greatest number of years of service, or in the event of action on the part of members of the military police or of any other section of the armed forces, the person who pursuant to the provisions laid down by or pursuant to article 67 of the Code of Military Penal Law is the superior.

3. In this Decree the following terms have the following meaning:

a. competent authority: the authority referred to in articles 12, 13 and 15 of the Police Act 1993;

b. force: every coercive use of force of more than minor significance used on persons or property;

c. use of force: the use of force and threatening the use of force, including taking a firearm to hand;

d. weapon:

1o. the equipment, arms and ammunition permitted pursuant to article 49, paragraph 1 of the Police Act 1993 which can be used to exercise force, and

2o. the equipment, arms and ammunition made available by Our Minister of Defence which can be used to exercise force in the performance of the police duties referred to in articles 6, 58, 59 and 60 of the Police Act 1993;

e. resources for deportation:

1. equipment for the deportation of aliens made available pursuant to article 49, Paragraph 1 of the Police Act 1993 to a police officer who is charged by or pursuant to the Aliens Act 2000 with guarding the borders or the supervision of aliens, and

2. equipment for the deportation of aliens made available by Our Minister of Defence, in conjunction with Our Minister of Alien Affairs and Integration to a member of the military police who is charged by or pursuant to the Aliens Act 2000 with guarding the borders or the supervision of aliens;

f. automatic firearm: firearm whereby several shots can be discharged with one pull of the firing mechanism or a firearm which can, by choice, discharge either one or several shots;

g. riot police: a unit of police officers as referred to in article 6 of the Control of Regional Police Forces Decree and the military police units charged with the same duties as those set out in the aforementioned decree;

h. doctor: the advising duty doctor;

i. special investigating officer: a speical investigating officer as referred to in article 142, paragraph 1 of the Code of Criminal Procedure;

j. the use of a firearm: pointing, keeping it pointed and actually using a firearm;

k. non-penetrating ammunition: ammunition which has been designed not to penetrate the body upon impact with a person.

4. In this Decree, detainee means the person who has been lawfully deprived of his liberty. detainee also means the person who has been placed in the custody of the police station or squad room in connection with assistance being given to them.

Article 2

An officer shall identify himself using the proof of ID given to him:

a. when acting in civilian clothing, without being so requested, unless exceptional circumstances make this impossible, and

b. when acting in uniform, upon request.

Article 3

An officer who provides assistance pursuant to the provisions of Chapter IX of the Police Act 1993 is under the command of the local competent authority or an officer designated by said authority.

CHAPTER 2. Force

§ 1. General

Article 4

The use of weapons is only permitted by an officer:

a. to whom such weapon is lawfully made available, insofar as he is acting in the performance of the duty for which the weapon was made available to to him, and

b. who is skilled in the use of such weapon.

Article 5

1. If the officer, in a closed-off area or otherwise, acts under the supervision of a superior present on site, he shall not use force until after having received an explicit order from said superior. The superior shall indicate which weapon shall be used.

2. Paragraph 1 does not apply in the event the superior referred to in paragraph 1 has stipulated otherwise in advance.

3. Nor does paragraph 1 apply in a case as referred to in article 10, paragraph 1.b, insofar as it would not have been reasonable to await the order.

Article 6

1. The police commissioner or the police officer designated by the police commissioner shall only deploy the unit referred to in article 6 or 8 of the Control of Regional Police Forces Decree after receiving the consent of the competent authority.

2. The officer designated by the competent authority shall only deploy the units referred to in articles 58 and 59 of the Police Act 1993 after receiving the consent of the competent authority.

§ 2. Firearms

Article 7

1. The use of a firearm, not being a firearm which is an automatic weapon or a long range precision rife, is only permitted:

a. to detain a person with regard to whom it can reasonably be assumed that he has a firearm on his person ready for immediate use and will use said firearm on people;

b. to detain a person who has escaped or attempted to escape detention, arraignment or other lawful deprivation of liberty, and who is suspected of or has been convicted of the commission of an offence

1°. which in its statutory definition is punishable by a custodial sentence of four years or more, and

2°. which forms serious harm to the physical integrity or personal life sphere, or

3°. which due to its consequence does or could pose a threat to society.

c. to control unrest or other serious disorder, if there is an order by the competent authority and an action in a closed-off area under the supervision of a superior;

d. to control military unrest, other serious military disorder or mutiny if members of the military police act on instruction of the Minister of Defence or the district attorney of Arnhem charged with military affairs in a closed-off area under the supervision of a superior.

2. The use of firearms in the cases referred to in paragraph 1 under *a* and *b* is only permitted against persons and transport vehicles in which or on which people are situated.

3. In the cases referred to in paragraph 1 under *a* and *b*, no use shall be made of firearms if the identity of the person to be detained is known and it can reasonably be assumed that postponement of the detention will not entail an unacceptable risk for the public order.

4. The commission of an offence as referred to in paragraph 1 under *b* includes attempt and the accessory forms referred to in articles 47 and 48 of the Penal Code.

Article 8

1. The use of an automatic firearm is only authorised against persons and against transport vehicles in which or on which persons are situated, in a situation in which there is an immediate, unlawful assault on one own's person or the person of another.

2. An automatic firearm may only be carried for training or for:

a. realising the detention of a person who may reasonably be assumed to be carrying a firearm which is ready for immediate use and and will use this against people,

b. the guarding and security of people and property.

3. The carrying of automatic firearms in the case referred to in paragraph 2, under *a*, is only permitted after receiving the consent of the district attorney and with the written authority of Our Minister of Justice. The authorisation shall be requested in writing through the *College van procureurs-generaal*. If the authorisation cannot be requested or granted in writing because of the requisite urgency, the authority can be requested and granted verbally. Verbal authorisation must be confirmed in writing within twenty-four hours. If possible the district attorney shall give the relevant mayor advance notice of the carrying of automatic firearms.

4. The carrying of automatic firearms in the case referred to in paragraph 2, under *b*, is only possible after receiving the consent of the competent authority and with the written authorisation of Our Ministers of Justice and of the Interior jointly. The competent authority shall request the authorisation in writing. If the authorisation cannot be requested or granted in writing because of the requisite urgency, the authority can also be requested and granted verbally. Verbal authorisation shall be confirmed in writing within twenty-four hours.

Article 9

1. The use of a long range precision rifle is only authorised in the event of very serious offences to prevent immediate danger to the lives of people.

2. Use of the weapon referred to in paragraph 1 shall take place under orders of the commander of a special unit (*bijstandseenheid*) as referred to in article 9 of the Control of Regional Police Forces Decree or in article 60 of the Police Act 1993.

3. A long range precision rifle may only be carried for training or for the actual combating of very serious offences whereby there are circumstances which pose an immediate threat to life.

4. The carrying of a long range precision rifle for the actual combating of very serious offences whereby there are circumstances which pose an immediate threat to life is only permitted after receiving the consent of the competent authority and with the written authorisation of Our Minister of Justice. The consent or the authorisation can be made subject to conditions. If the authorisation cannot be requested or granted in writing because of the requisite urgency, it can be requested and granted verbally. Verbal authorisation must be confirmed in writing within twenty-four hours.

Article 10

1. An officer may only take a firearm, not being an automatic firearm or long range precision rifle, to hand:

a. in cases in which the use of a firearm is permitted, or

b. in connection with his safety or that of others, if it can reasonably be assumed that a situation will arise in which he is authorised to use a firearm.

2. If a situation as referred to in paragraph 1.b has not arisen or has ceased, the officer must immediately put away the firearm.

Article 10a

1. An officer shall give a warning immediately before he aims and discharges a firearm, not being a long range precision rifle, in a loud voice or in some other unmistakable manner that shots will be fired if the order is not immediately followed. This warning, which can if necessary be replaced by a warning shot, need not be given if the circumstances do not allow for a warning.

2. A warning shot must be given as much as possible in such manner that danger to people or property is avoided as much as possible.

§ 2a. Non-penetrating ammunition

Article 11

Articles 7 through 10a do not apply to the use and handling of a firearm which is loaded with non-penetrating ammunition.

Article 11a

The use of a firearm which is loaded with non-penetrating ammunition is only permitted:

a. to detain a person who may reasonably be assumed to be carrying a weapon ready for immediate use and that he will use the weapon against people; or

b. to detain a person who has avoided or attempted to avoid his detention, arraignment or other lawful deprivaiton of liberty.

Article 11b

An officer shall give a warning immediately before he aims and discharges a firearm which is loaded with non-penetrating ammunition, in a loud voice or in some other unmistakable manner that shots will be fired, if the order is not immediately followed. This warning need not be given if the circumstances do not permit a warning to be given.

Article 11c

Articles 11a and 11b apply mutatis mutandis if the non-penetrating ammuniation is discharged by means of an item other than a firearm.

§ 2b. Pepper spray

Article 12a

1. The use of pepper spray is only permitted:
a. to detain a person who may reasonably be assumed to be carrying a weapon ready for immediate use and that he will use this weapon against a person;
b. to detain a person who has avoided or attempted to avoid detention, arraignment or some other lawful deprivation of liberty;
c. as a defence against or to control aggressive animals.
2. Pepper spray shall not be used against:
a. persons who are visibly younger than 12 or older than 65 years of age;
b. women who are visibly pregnant;
c. persons against whom use could be disproportionately harmful as a result of a respiratory or other serious health ailment which is visible to the officer;
d. groups of people.

Article 12b

An officer shall issue a warning immediately before he aims pepper spray at and uses pepper spray against a person, in a loud voice or in some other unmistakable manner that pepper spray will be used if the order is not immediately followed. This warning need not be given if the circumstances do not reasonably allow the warning to be given.

Article 12c

Pepper spray shall be used against a person a maximum of two times per incident for a duration of no longer than approximately one second and at a distance of at least one metre.

§ 3. Other weapons

Article 13

1. The use of CS tear gas is only permitted:
a. in enclosed spaces to detain a person if it can reasonably be assumed that said person is carrying a firearm ready for immediate use and will use said weapon against persons or will use other life-threatening force against people;
b. other than in enclosed spaces to disperse gatherings or crowds which form a serious and immediate threat to the safety of persons and property.
2. The use of CS tear gas is only permitted on instruction of the superior after receiving the prior consent of the competent authority.
3. The superior who ordered the use of CS tear gas shall stipulate in the order how many CS tear gas granades are to be used.

Article 14

The use of a water cannon is only permitted when the riot squad is acting on instruction of the superior and after obtaining the consent of the competent authority.

Article 15

1. The use of a police guard dog is only permitted under the direct and continual supervision of a handler:

a. with the patrol service, and

b. in the event of action of the riot squad after receiving the consent of the competent authority.

2. The handler must possess a certificate issued in accordance with article 49, paragraph 1 of the Police Act 1993.

Article 16

The use of an electric stun gun is only permitted as a means of defence against aggressive animals after receiving the superior's consent.

§ 4. Reporting the use of force

Article 17

1. An officer who has used force must immediately report the relevant facts and circumstances, as well as the consequences thereof, to his superior.

2. The superior shall immediately record the report referred to in paragraph 1 in a manner established by Our Ministers of Justice and of the Interior and Kingdom Relations by ministerial regulation.

3. The police commissioner shall give notice of the report referred to in paragraph 2 within 48 hours to the district attorney of the district within which force has been used, or the commander of the military police shall give such notice to the district attorney of Arnhem charged with military affairs in the event the matter involves military personnel, if:

a. the consequences of the use of force give rise to such in the opinion of the police commissioner or the commander,

b. the use of force has caused physical injury of more than minor significance or has resulted in death, or

c. use has been made of a firearm and one or more shots were discharged from the firearm.

Article 18

[Repealed.]

Article 19

The superior shall inform the officer as soon as possible as to the handling of the report. Upon request the officer shall be given interim information.

CHAPTER 3. Search of clothing

Article 20

1. The search referred to in article 8, paragraph 3 of the Police Act 1993 shall be effected by going over the surface of the clothing and shall be executed as much as possible by an officer of the same gender as the person who is subjected to the search.
2. The search referred to in article 8 paragraph 4 of the Police Act 1993 shall be executed by an officer of the same gender as the person who is subjected to the search.

Article 21

An officer who has carried out a search as referred to in article 8, paragraph 3 or 4 of the Police Act 1993 shall immediately report this to the superior in writing, stating the reasons which led to the search.

CHAPTER 4. Handcuffs

Article 22

1. An officer can place handcuffs on a person who has been lawfully deprived of his liberty for the purpose of transportation.
2. The measure referred to in paragraph 1 can only be taken if the facts or circumstances reasonably require such with an eye on the risk of escape, or with an eye on danger to the safety or life of the person who has been lawfully deprived of his liberty, of the officer or of third parties.
3. The facts and circumstances referred to in paragraph 2 can only be related to:
a. the person who has been lawfully deprived ofhis liberty, or
b. the nature of the offence on the basis of which the deprivation of liberty has taken place, in conjunction with the way in which and the situation in which the transport took place.

Article 23

An officer who makes use of handcuffs as referred to in article 22, paragraph 1 shall immediately give written notice thereof to the superior, stating the reasons which led to the use of handcuffs.

CHAPTER 4A. Resources for the deportation of aliens

Article 23a

1. An officer who by or pursuant to the Aliens Act 2000 is charged with guarding the border or with the supervision of aliens can restrict the freedom of movement of an alien upon his deportation by airplane, in order to ensure the proper execution of the deportation.
2. The measure referred to in paragraph 1 can only be taken if:
a. the facts or circumstances reasonably require such with an eye on the risk of escape, or with an eye on the risk to the safety or the life of the alien, of the officer or of third parties, or with an eye on the risk of a serious breach of the public order, and
b. the use of the resource cannot reasonably cause any risk to the alien's health.

3. If the officer referred to in paragraph 1 acts under the supervision of a superior on site, he shall only make use of resources for deportation after receiving an explicit order from the superior. The superior shall indicate in this respect what resource is to be used.
4. The use of a resource for deportation is only permitted by an officer skilled in the use of such resource.

Article 23b

1. An officer who has made use of a resource for deporation as referred to in article 23a, paragraph 1 with regard to an alien who is deported, shall immediately report this to his superior in writing, stating the nature of the resource, the reasons which led to the use and the consequences ensuing therefrom.
2. The superior shall make a record of the report referred to in paragraph 1.

CHAPTER 5. Assistance

Article 24

1. An officer shall see to it that people with minor wounds, symptoms of illness and people with regard to whom there is doubt on this point are referred to a GP or an emergency department of a hospital. If necessary, the officer shall mediate in obtaining suitable transport.
2. The officer shall see to it that people with serious wounds and unconcious people, including people who cannot be woken up or who are not coherent, are taken to hospital by ambulance. The officer shall give information regarding the nature and circumstances of the event which led to such condition, and the medical details and medicines found on a person to the medical care providers.

Article 25

1. The officer shall endeavour to ensure that people who due to being under the influence of alcohol or due to other causes form an immediate danger, be such to the public order, safety or health, or to himself, are removed from public places as referred to in article 1 of the Public Manifestations Act in the most suitable manner. Public places includes transport vehicles which are located at these places, insofar as they are not being used as a dwelling.
2. The officer shall hand over people as referred to in paragraph 1 to the own care providers, insofar as the circumstances permit such. In the event of lack of care facilities elsewhere, by way of assistance they can be placed at the police station or squad room if this is necessary for their protection and this is not against their will.
3. The officer shall alert the doctor as to persons as referred to in paragraph 1, who are known to be or appear to be mentally disturbed, after attempting to contact the relevant person's own GP if possible.

CHAPTER 6. Measures vis-a-vis detainees

§ 1. General

Article 26

1. The officer shall treat the detainee in accordance with the provisions laid down by or pursuant to article 15 of the Control of Regional Police Forces Decree.
2. The officer shall record the details stipulated pursuant to article 15, paragraph 6 of the Control of Regional Police Forces Decree.

Article 27

1. Insofar as such is not contrary to the provisions laid down by or pursuant to the Code of Criminal Procedure, the officer shall inform a family member or a housemate of the detainee as soon as possible of the incarceration. In the event the detainee is a minor, the officer shall do so of his own accord, if the detainee is of age, the officer shall only do so upon the detainee's request.
2. If the circumstances do not permit implementation of paragraph 1 in respect of a detainee who is not a resident, the embassy or the consulate of the country in which the detainee is a resident shall be informed of the incarceration.

§ 2. Taking clothing and objects into custody

Article 28

1. An officer shall search the detainee immediately prior to incarceration at the police station or squad room, by frisking and searching his clothing for the presence of objects which during incarceration could form a danger to the safety of the detainee or others.
2. If the officer finds objects as referred to in paragraph 1, the officer shall take these into custody.
3. The search referred to in paragraph 1 shall be executed where possible by an officer of the same gender as the person who is subjected to the search.

Article 29

1. The officer can only demand of the detainee that he take off his clothes if:
a. during incarceration the clothing can form a danger to the safety of the detainee or to others and an assistant district attorney has granted consent therefore;
b. in the opinion of the doctor, during the incarceration the clothing can form a danger to the health of the detainee or others.
2. The officer shall take custody of the clothing referred to in paragraph 1 and shall provide replacement clothing.

Article 30

1. An officer who has carried out a search as referred to in article 28, paragraph 1 shall immediately prepare a written report hereof for the superior.
2. The officer shall precisely record all objects and items of clothing which he has taken into custody. A general description shall suffice for objects which are small in size and value.

3. A copy of the record referred to in paragraph 2 shall be signed by the detainee and the officer and handed over to the detainee.

§ 3. Permanent video surveilliance

Article 31

1. After receiving the consent of the assistant district attorney, the officer can subject the detainee to permanent video survelliance.
2. The measure referred to in paragraph 1 is only permitted in those cases in which there is such risk of danger to the life or the safety of the party in question that continuous observation is necessary to avoid this risk.
3. The officer shall inform the person in question of the permanent video surveilliance and shall make a record of the permanent video surveilliance.

§ 4. Medical assistance

Article 32

1. In the event there are indications that a detainee requires medical assistance or if medicines have been found with this person, the officer shall consult with the doctor. The officer shall also consult with the doctor if the detainee himself requests medical assistance or medicines.
2. In the event the detainee requests medical assistance from his own doctor, the officer shall inform the doctor thereof.
3. In the event the detainee indicates he does not wish to have any medical assistance, while there are indications that medical assistance is required, the officer shall inform the doctor and he shall inform the doctor of the detainee's attitude.

Article 33

The officer may not impose any restrictions on the doctor in the examination and treatment. He shall follow the doctor's instructions regarding the detainee's care and shall make a record of the instructions given by the doctor.

Article 34

1. The officer shall inspect the detainee regularly on the understanding that:
a. in the event the doctor has been alerted, the detainee shall be checked up on in his cell at least every fifteen minutes;
b. in the event medical assistance has been given, the detainee shall be checked up on as often as the doctor has prescribed;
c. in the event no medical assistance is deemed necessary, the detainee shall be checked up on once every two hours.
2. In the cases referred to in paragraph 1 under *a* and *b*, the officer shall check the cell and the person, whereby he shall pay particular attention to the degree in which the detainee can be woken up and is coherent. Persons who are in a condition in which they cannot be woken up or are not coherent, shall immediately be taken to a hospital by ambulance.
3. The officer shall register the observations referred to in paragraph 1.

Article 35

When transferring the detainee the officer shall send along the medicines, the records referred to in articles 26, paragraph 2, 33 and 34, paragraph 3, insofar as these may be relevant, and the doctor's reports which are intended for a doctor who will be taking over treatment of the detainee.

§ 5. Release

Article 36

The officer shall see to it that when a person is released, if such person cannot make his own way around, there will be transport and supervision for such person.

CHAPTER 7. Special investigating officer

Article 37

1. If Our Minister of Justice, pursuant to article 8, paragraph 7 of the Police Act 1993 has stipulated that a special investigating officer has the authority to exercise the powers referred to in paragraphs 1 and 3 of said article, the special investigating officer in question shall act in accordance with articles 5, 17, 19, 20, paragraph 1 and 21 of this Decree. In article 17, paragraph 3, "the commissioner" is to read: the superior.

2. If the instruction also encompasses the use of a weapon, a guard dog or handcuffs, the special investigating officer in question shall act in accordance with articles 4, 7, paragraph 1, beginning and under *a* and *b*, paragraphs 2, 3 and 4, 10, 10a, 12a, 12b, 12c, 15, paragraph 1, beginning and under *a*, and paragraph 2, 16, 22 and 23 of this Decree.

3. For the application of paragraphs 1 and 2, the following terms have the following meaning:

a. competent authority: the authority referred to in article 13 of the Police Act 1993;

b. the superior: the direct supervisor, referred to in article 1 of the Special Investigating Officer Decree.

c. weapon: the arms, ammunition and equipment which can be used to exercise force which are permitted pursuant to article 3a, paragraphs 1 through 3 of the Arms and Ammunition Act.

Article 38

Special investigating officers who are authorised to use a weapon or handcuffs shall only make use of weapons or handcuffs prescribed by Our Minister of Justice when performing their duties.

Article 39

Special investigating officers do not have the authority to exercise the powers referred to in Article 8, paragraphs 1 and 3 of the Police Act 1993 until after said authority has been recorded on the oath and the officer in question has demonstrated his skill in the performance thereof.

CHAPTER 8. Final provisions

Article 39a

In agreement with Our Minister of Justice, within three years after the entry into force of the decree of 25 August 2006 to amend the Official Instruction for the police, the military police and special investigating officers in connection with the introduction of non-penetrating ammunition (Stb. 2006, 407), Our Minister of the Interior and Kingdom Affairs shall present the States-General with a report on the effectiveness and the effects of articles 11 through 11c in practice.

Article 40

This decision enters into force as of the day when the Police Act 1993 enters into force.

Article 41

This decree shall be cited as: Official Instruction for the Police, the Military Police and Special Investigating Officers.

Order that this decree and the related explanatory notes shall be publised in the *Staatsblad* (Bulletin of Acts, Orders and Decrees).

The Hague, 8 April 1994

Beatrix

The Minister of Justice,
E. M. H. Hirsch Ballin

The Minister of the Interior,
E. van Thijn

Published Twenty-One April 1994

The Minister of Justice,
E. M. H. Hirsch Ballin

SPAIN

Spain authorized the use for other police forces Prüm partners similar equipment in the frame of joint operations or urgent situations. If this normal equipment would be very different is mandatory a expressed authorization.

The chapters 5 and 6 of the Treaty establish as general principle the subordination to the national law of host territory, the application by analogy of responsibility regime collected in the 43 article of Application Agreement of Schengen Treaty – article 30 of Treaty – and the assumption of the measure to the State of territory, article 25.5 of the Treaty.

If the Spanish Police officers has legal restriction to carry on and use of some weapons, the same restrictions affect the police officers of the other contracting party that acts in Spanish territory. The Spanish national law asses:

1.- The absolute ban for all – civilians and police officers – of possession and use, of next types of weapons:

a. The firearms that have been modified their characteristics substantially without authorization.
b. The long weapons that contain special devices, in their breech or mechanisms to house guns or other weapons.
c. The guns and revolvers that take adapted a small breech.
d. The firearms to house or housed inside sticks or other objects.
e. The firearms feigned low appearance of any other object.
f. The stick-rapier, the daggers of any class and the automatic knives. They will be considered daggers the cut and thrust weapons with a blade smaller than 11 centimeters, double bits and pointed.
g. The firearms, pressurized air or another compressed gas, combined with cut and thrust weapons.
h. The truncheon made of wire or lead; the brainteaser ; the "llaves de pugilato", with or without spikes; the slingshot and perfected "blowpipe"; the "munchacos" and "xiriquetes", as well as any other specially dangerous instruments for the physical integrity of the people.

2.- It is forbidden except for especially qualified civil servant (police officers among others): (1)

a. The semiautomatic weapons of 2.2.and 3.2 categories whose capacity of freight were up of 5 shotgun shell, the housed in the breech included, or whose breech were removable.
b. The self defense sprays and all those weapons that discharge gases or aerosols, and any device with mechanisms able of throw toxic or corrosive narcotics.
c. The electric or rubber truncheon or similar.
d. The applicable mufflers to firearms.
e. The cartridge with "piercing bullets", explosive, incendiaries bullets, as well as the corresponding projectiles.
f. The ammunition for guns and revolvers with projectiles "dum-dum" or "hollow peak", as well as the own projectiles.
g. The long firearms give clipped canyons.

(1) The characteristics of caliber, weight and diameter or gas authorized in Spain were given to the presidency. In the present document, appear a scheme of the basic equipment for Spanish police officers.

3.- Spain consider weapons of war, reason why only can be used by the police officers when the Spanish Government has authorized the next:

a. Firearms or systems with caliber equal or superior to 20 millimeters.

b. Firearms or weapon systems with lower caliber to 20 millimeters whose caliber were considered by the Ministry of Defense like of war.
c. Automatic firearms.
d. The ammunition for the weapons indicated in the sections a) and b).
e. Bombs of aviation, missiles, rockets, torpedos, mines, grenades, as well as their fundamental pieces.
f. Those not included in the previous sections and that they are considered like weapons of war for the Department of Defense.

RULES OF SELF-DEFENSE

In Spain we consider that someone acts under legitimate defense when he acts in defense of person or own or others people rights, whenever concur the next requirements:

Defense of people.-

1.- Unlawful aggression
2.- Rational necessity of used mean to avoid it or repel it
3.- Lack of enough provocation for the part of defender

Defense of goods.-

In case of defense of goods, it reputes unlawful aggression the attack over them when this is felony or fault and the goods became in serious danger of deterioration or imminent miss.

Defense of a house (place where someone lives in).-

In case of defense of house or it departments, it reputes unlawful aggression the undue entrance there.

For that, house is all closed space dedicated by the resident to develop in a effective way one human activity with exclusion of other people."

„Végrehajtási megállapodás

a Belga Királyság, a Németországi Szövetségi Köztársaság a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között a határon átnyúló együttműködés fokozásáról, különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció elleni küzdelem terén 2005. május 27-én Prümben (Németország) aláírt Szerződéshez

1. szakasz: Cél és meghatározások

1. Cél

A Szerződés 44. cikke szerint ezen Végrehajtási megállapodás célja, hogy a Szerződés adminisztratív és technikai végrehajtásához és alkalmazásához szükséges rendelkezéseket meghatározza.

2. Meghatározások

A Végrehajtási megállapodás vonatkozásában:

2.1 „Szerződés” alatt a Belga Királyság, a Németországi Szövetségi Köztársaság a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között a határon átnyúló együttműködés fokozásáról, különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció elleni küzdelem terén 2005. május 27-én Prümben (Németország) aláírt Szerződés értendő;

2.2 „Fél” alatt a Szerződés egy olyan Szerződő Fele értendő, amely ezt a Végrehajtási megállapodást aláírta;

2.3 A Szerződés 3., 4. és 9. Cikkében hivatkozott „keresés”, „összehasonlítás” vagy „összehasonlítással végzett keresések” alatt azon eljárásokat kell érteni, amelyek révén megállapítják, hogy van-e egyezés azon DNS- illetve ujjnyomat-adatok, amelyeket egy Fél közölt, és az egy, több vagy az összes többi Fél adatbázisában tárolt adat közt;

2.4 A „DNS-profil” olyan betű- vagy számkód, amely egy elemzett emberi DNS-minta – vagyis az egyes vegyi képletek a különböző DNS-helyeken (lókuszok) – nem kódolt régiójának azonosító jelölés-készletét jelöli;

2.5 A „DNS nem kódolt régiója” alatt azokat a kromoszóma-zónákat értjük, amelyek nem hordoznak genetikai kifejezést, azaz ismereteink szerint nem nyújtanak információt konkrét öröklött tulajdonságokról;

2.6 A „DNS referencia-adat” alatt egy DNS-profil és a hozzá kapcsolódó nem DNS-specifikus adat értendő;

2.7 A „nem DNS-specifikus adat” tartalmaz:

2.7.1 egy olyan azonosító kódot vagy számot, amely egyezés esetén lehetővé teszi a Felek számára, hogy személyes adatot és/vagy egyéb információt tölthessenek le adatbázisukból, azzal a céllal, hogy azt átadják egy, több vagy az összes többi Félnek, a Szerződés 5. Cikke alapján;

2.7.2 egy Félkódot, amely a DNS-profil nemzeti eredetét jelöli, és

2.7.3 egy, a Szerződés 2. Cikk (2) bekezdése szerint a Felek által megnevezett DNS-profil típusát jelölő kódot;

2.8 „azonosítatlan DNS-profil” alatt a bűncselekmények nyomozásából származó, egy még nem azonosított személyhez tartozó biológiai anyagmaradványból nyert DNS-profil értendő;

2.9 a szakkifejezésként használt „DNS referencia-profil“ alatt a Szerződés 2. Cikk (3) bekezdése alapján a nemzeti DNS-elemzési adatbázisban tárolt, azonosított személy DNS-profilja értendő;

2.10 „ujjnyomat-adat” alatt ujjnyomat-képek, ujjnyomat látens képei, tenyérnyomatok, tenyérnyomatok látens képei, valamint ezen képek sablonjai (*minutiae*) értendők, amennyiben ezeket automatizált adatbázisban tárolják és kezelik;

2.11 „további megkeresés” alatt egy Félnek egy, több vagy az összes többi Félhez az összehasonlított DNS- vagy ujjnyomat-adat egyezése esetén intézett megkeresés értendő, melynek célja további személyes adat vagy egyéb információ szerzése a Szerződés 5. és 10. Cikke szerint;

2.12 „gépjármű-nyilvántartási adat” alatt a C.1. Mellékletben meghatározott adatkészlet értendő, amelynek az alábbi, 2.13-as pontban meghatározott automatizált keresési eljárás céljából való kölcsönös hozzáférhetővé tételéről a Felek megegyeztek;

2.13 „automatizált keresés” alatt az az online hozzáférési eljárás értendő, amelynek célja a Szerződés 33. Cikk (1) bekezdésének 2. pontja alapján az egyik, több, vagy az összes többi Fél adatbázisába való betekintés;

2.14 „a 12. Cikk szerinti rendszer” alatt mindazon technikai intézkedés és funkcionális aspektus (mint pl. hálózat, interfészek, biztonsági kérdések) értendő, amelyet a Szerződés 12. Cikke szerinti gépjármű-nyilvántartási adatok cseréje érdekében hoztak létre;

2.15 „EUCARIS” alatt az Európai Gépjármű- és Vezetői Engedély Információs Rendszer értendő, amelyet a 2000. június 29-én Luxemburgban aláírt vonatkozó szerződéssel hoztak létre;

2.16 a Szerződés 3. Cikk (1) bekezdésében, 9. Cikk (1) bekezdésében és 12. Cikk (1) bekezdésében említett „egyedi esetek” alatt egyetlen nyomozati vagy bűnüldözési ügyirat értendő. Amennyiben ez az ügyirat egynél több DNS-adatot, ujjnyomat-adatot vagy gépjármű-adatot tartalmaz, ezeket együttesen, egy keresési lekérdezésként is lehet továbbítani;

2.17 az „adatkeresés vagy –átadás oka” alatt a Szerződés 39. Cikkének alkalmazása során az a jelölés értendő, amely egyértelmű kapcsolat létrehozását teszi lehetővé egy adott megkeresés és azon ennek megfelelő egyedi eset között, amely a megkeresés alapjául szolgált;

2.18 a „TESTA II kommunikációs hálózat” alatt az Európai Bizottság által kezelt „Közigazgatásközi Transzeurópai Telematikai Szolgáltatások” („*Trans European Services for Telematics between Administrations*”) értendőek, valamint ezek bármely módosított változata.

2. szakasz: DNS-profilok

3. DNS-profilok összeállítása és összehasonlítása

3.1 A Szerződés 2. Cikkének végrehajtása céljából a Szerződés alapján kicserélendő DNS-referenciadatok egy DNS-profilból és a nem DNS-specifikus adatokból állnak.

3.2 Az A Mellékletben meghatározott közös műszaki specifikációk (beleértve az egyezési szabályokat, az algoritmusokat és a Félkódszámokat) készletét a Felek nemzeti kapcsolattartó pontjain telepítik és alkalmazzák minden, a DNS-profiloknak a 3.1 pontban hivatkozott keresésével és összehasonlításával kapcsolatos lekérdezés és válasz esetén.

3.3 A DNS-profilokat az A Mellékletben meghatározott osztott jelölők alapján kell összehasonlítani. Bármely, a kérelmező Fél által keresés vagy összehasonlítás céljából átadott DNS-profilt össze kell hasonlítani minden, a megkeresett Fél által a Szerződés 2. Cikk (2) és (3) bekezdése alapján rendelkezésre bocsátott DNS-profillal.

3.4 A Felek a létező szabványokat használják, mint pl. az Európai Szabványkészletet (*European Standard Set* – ESS) vagy az Interpol Lókusz-szabványkészletet (*Interpol Standard Set of Loci* – ISSOL).

4. DNS-kérési és jelentési szabályok

4.1 A Szerződés 3. és 4. Cikkében hivatkozott automatizált keresés vagy összehasonlítás iránti kérés kizárólag az alábbi információkat tartalmazhatja:

4.1.1 a kérelmező Fél Félkódja;
4.1.2 a kérelem dátuma, időpontja és hivatkozási száma;
4.1.3 a DNS-profilok és ezek nem DNS-specifikus adatai;
4.1.4 az átadott DNS-profilok típusa (azonosítatlan DNS-profilok vagy DNS-referenciaprofilok)

4.2 A Felek biztosítják, hogy a kérések teljes mértékben eleget tegyenek a Szerződés 2. Cikk (3) bekezdésében foglalt és az A.3. Mellékletben megismételt nyilatkozatokban rögzített feltételeknek.

4.3 A 4.1. pontban említett kérelemre adott választ (egyezési jelentés) a kérelmező Fél nemzeti kapcsolattartó pontjának kell elküldeni, annak megállapítása érdekében, hogy szükség van-e további lekérdezésre. Az egyezési jelentés kizárólag az alábbi információkat tartalmazhatja:

4.3.1 annak jelzését, hogy volt-e egy vagy több egyezés („találat”), avagy nem („nincs találat”);
4.3.2 a kérelem dátuma, időpontja és hivatkozási száma;
4.3.3 a válasz dátuma, időpontja és hivatkozási száma;
4.3.4. a megkeresett Fél Félkódja;
4.3.5 a kérelmező Fél és a megkeresett Fél nem DNS-specifikus adatai;
4.3.6 az átadott DNS-profilok típusa (azonosítatlan DNS-profilok vagy DNS-referenciaprofilok);
4.3.7 a Szerződés 4. Cikke szerinti összehasonlítás esetén az egyeztetett DNS-profil.

4.4 Találatról automatizált értesítést csak abban az esetben kell adni, ha az automatizált keresés vagy összehasonlítás az A.1. Mellékletben meghatározott minimális számú lókusz egyezését eredményezte. A Szerződés 3. Cikke szerinti ellenőrzési célú keresés esetén a Felek nemzeti kapcsolattartó pontjai meghozzák a nemzeti jogukkal összhangban álló megfelelő intézkedéseket.

5. A DNS-adatok továbbítására szolgáló kommunikációs hálózat

A DNS-vonatkozású adatok elektronikus cseréje a Felek közt a „TESTA II” kommunikációs hálózat használatával történik az A.5. Mellékletben rögzített műszaki specifikációknak megfelelően.

6. Minőség-ellenőrzési intézkedések

A Felek megfelelő intézkedéseket tesznek a más Felek számára hozzáférhetővé tett, vagy összehasonlításra átadott DNS-profilok sértetlenségének garantálására. Ezeknek az intézkedéseknek összhangban kell állniuk a nemzetközi szabványokkal, mint pl. az ISO 17025. Ezen DNS-profilok bűnügyi technikai aspektusai meg kell, hogy feleljenek az A.1. Mellékletben rögzített specifikációknak.

3. szakasz: Ujjnyomat-adatok

7. Ujjnyomat-adatok átadása

7.1 A Szerződés 9. Cikkének végrehajtása céljából a Felek megteremtik a kölcsönösen hozzáférhető műszaki belépés lehetőségét „automatizált ujjnyomat-azonosító rendszereikhez” (a továbbiakban: „AUAR”).

7.2 A 7.1. pontban említett rendszerek csak a bűncselekmények megelőzésére és nyomozására létrehozott automatizált ujjnyomat-azonosító rendszereket jelentik. A közigazgatási nyilvántartásokban szereplő adatokat nem szabad átadni.

7.3 Az ujjnyomat-adatok digitalizálása és más Felek számára történő átadása a B.1. Mellékletben leírt „Interfész-ellenőrzési dokumentumban” („*Interface Control Document* – ICD”) specifikált adatformátumnak megfelelően történhet. Minden Félnek biztosítania kell, hogy a más Felek által átadott adatokat össze lehessen hasonlítani saját AUAR-juk referencia-adataival.

7.4 A Szerződés 9. Cikkében hivatkozott referenciák lehetővé teszik az egy személynek vagy egy esetnek való egyértelmű megfeleltetést, valamint a kérelmező Fél azonosítását.

8. Az eredmények keresése és átadása

8.1 A Felek biztosítják, hogy az átadott ujjnyomat-adatok megfelelő minőségűek az AUAR általi összehasonlításhoz. A megkeresett Fél haladéktalanul, egy automatizált eljárással ellenőrzi az átadott ujjnyomat-adatok minőségét. Amennyiben az adat nem alkalmas az automatizált összehasonlításra, a megkeresett Fél haladéktalanul értesíti erről a kérelmező Felet.

8.2 A megkeresett Fél abban a sorrendben hajtja végre a kereséseket, amilyenben a kéréseket megkapta. A kéréseket 24 órán belül kell feldolgozni, egy teljesen automatizált eljárással. A kérelmező Fél, amennyiben a nemzeti joga ezt megköveteli, kérheti ezen keresések gyorsított végrehajtását. Ezeket a kereséseket a megkeresett Fél haladéktalanul végrehajtja. Ha a megkeresett Félnek fel nem róható okokból a határidő nem tartható, az összehasonlítást haladéktalanul el kell végezni, amint ennek akadályai elhárultak.

8.3 A megkeresett Fél gondoskodik arról, hogy a rendszer képes legyen teljesen automatizált módon haladéktalanul átadni bármilyen „találat” vagy „nincs találat” jelzést a kérelmező Fél számára. Találat esetén átadja az ujjnyomat-adatokat és a Szerződés 9. Cikk (2) bekezdésében említett referenciákat minden ujjnyomatadat-egyezés esetén.

9. Az ujjnyomat-adatok átadására szolgáló kommunikációs hálózat

Az ujjnyomat-vonatkozású adatok elektronikus cseréje a Felek közt a „TESTA II” kommunikációs hálózat használatával történik az A.5. Mellékletben rögzített műszaki specifikációknak megfelelően.

10. Az ujjnyomat-adatok automatizált keresésének meghatározása és kapacitásai

10.1 A B.2. Melléklet rögzíti az ujjnyomat-adatok (jelöltek) különböző típusainak ellenőrzésre elfogadott átadásonkénti maximumát.

10.2 A B.3. Melléklet rögzíti minden Fél esetében az azonosított személyek ujjnyomat-adataira vonatkozó keresések napi maximumát.

10.3 A B.4. Melléklet rögzíti minden Fél esetében az ujjnyomat-nyomok utáni keresési kapacitás napi maximumát.

4. szakasz: Gépjármű-nyilvántartási adatok

11. Keresési eljárás és az adatok átadása

11.1 A Szerződés 12. Cikkének céljaira a Felek létrehozzák a nemzeti kapcsolattartó pontok hálózatát, hogy automatizált kereséseket hajtsanak végre saját gépjármű-nyilvántartási adatbázisaikban. A C.3. Melléklet rögzíti az adatcsere műszaki feltételeit.

11.2 A Szerződés rendelkezéseinek sérelme nélkül, és figyelembe véve különösen a 38. és a 39. Cikk rendelkezéseit, a Felek – kérelmező és megkeresett Félként eljárva – megszervezik saját nemzeti kapcsolattartó pontjaik működési rendjét, a Szerződés rendelkezéseinek és alapelveinek szellemében.

11.3 A teljes mértékben automatizált kérelmezési eljárást választó Feleknek biztosítaniuk kell, hogy minden kérelem áthaladjon a Szerződés által előírt saját nemzeti kapcsolattartó pontjukon, amelynek egy felelős tisztségviselő felügyelete alatt kell állnia.

12. A gépjármű-nyilvántartási adatok átadására szolgáló kommunikációs hálózat

12.1 A gépjármű-nyilvántartási adatok elektronikus cseréjének eszközéül a Felek a „TESTA II” kommunikációs hálózatot választják, a 12. Cikk szerinti rendszer céljaira kifejlesztett EUCARIS szoftvert, illetve e két rendszer bármilyen módosított változatát.

12.2 Minden, a 12. Cikk szerinti rendszer – köztük az EUCARIS-technológia – kezeléséből és használatából eredő megosztandó költséget évente kell megvitatni és abban megállapodni.

13. A személyes adatok és az adatbiztonság védelmét célzó műszaki és szervezési intézkedések

A Szerződés 38. Cikk (2) bekezdésében említett automatizált keresés adatvédelmet, biztonságot, bizalmasságot és sértetlenséget érintő műszaki specifikációját, a hálózati rejtjelezést és engedélyezési eljárásokat, valamint az automatizált keresésekhez való hozzáférési jogosultság ellenőrzési eljárásait a C.2. Melléklet rögzíti.

5. szakasz: Rendőri együttműködés

14. Közös műveletek

14.1 Két vagy több Fél egy missziós nyilatkozattal indíthat el egy, a Szerződés 24. Cikkében leírt közös műveletet. A művelet megkezdése előtt írásban vagy szóban megállapodnak az alábbi operatív feltételekben:

a) a missziós nyilatkozatban részes Felek kompetens hatóságai;
b) a művelet konkrét célja;
c) a fogadó állam, ahol a művelet lezajlik;
d) a fogadó állam azon földrajzi területe, ahol a művelet lezajlik;
e) a művelet missziós nyilatkozatában rögzített időkeret;
f) a küldő állam által a fogadó államnak nyújtandó konkrét segítségnyújtás, beleértve a tiszteket, vagy más hivatalos személyeket, tárgyi és pénzügyi segítséget;
g) a műveletben részt vevő tisztek;
h) a műveletért felelős tiszt;
i) a küldő állam tisztjeinek és más hivatalos személyeinek a fogadó államban a művelet során gyakorolható jogai;
j) az egyes fegyverek, lőszerek és felszerelés, amelyet a kiküldött tisztek a művelet során, a D.3. Mellékletben meghatározott szabályok szerint használhatnak;
k) a szállítás, az elszállásolás és a biztonság logisztikai feltételei;
l) a közös művelet költségeinek viselése, ha ez eltér a Szerződés 46. Cikkében rögzítettektől;
m) bármi egyéb lehetséges tisztázandó körülmény.

14.2 Bármely Fél kompetens hatósága kezdeményezheti egy közös művelet elindítását. A D.1. Mellékletben bármely Fél rögzítheti a beérkező kérések feldolgozására vonatkozó eljárást. Ha nincs rögzített eljárás, a D.1. Melléklet szerint kijelölt nemzeti kapcsolattartó pont nyújt segítséget a többi Félnek, hogy kérésüket a kompetens hatósághoz juttathassák el.

15. Határon átnyúló műveletek közvetlen veszély esetén

15.1. A D.2. Melléklet rögzíti a Szerződés 25. Cikk (3) bekezdése értelmében haladéktalanul értesítendő hatóságok körét.

15.2 Ezen hatóságok elérhetőségeiben bekövetkezett bármely változásról a többi Félnek a D.2. Mellékletben felsorolt nemzeti kapcsolattartó pontját a lehető leghamarabb tájékoztatni kell.

16. Fegyverek, lőszerek és felszerelés szállítása

A D.3 Mellékletben minden Fél felsorolja azokat a fegyvereket, lőszereket és felszereléseket, amelyeket a Szerződés 28. Cikk (1) bekezdés harmadik mondata értelmében tilos szállítani, a fegyvereket, lőszereket és felszereléseket, amelyeket tilos használni és ennek jogi feltételeit, a Szerződés 28. Cikk (2) bekezdése értelmében, valamint a Szerződés 28. Cikk (5) bekezdése szerinti gyakorlati feltételeket.

6. szakasz: Általános rendelkezések

17. A Szerződés és a Végrehajtási megállapodás alkalmazásának és végrehajtásának értékelése

17.1 A Szerződés és a Végrehajtási megállapodás adminisztratív és technikai alkalmazásának és végrehajtásának értékelését a Szerződés 43. Cikk (2) bekezdése alapján létrehozott Közös Munkacsoport, vagy a Közös Munkacsoport által ezzel megbízott bármilyen technikai munkacsoport végzi. Erre az értékelésre bármely Fél kérése alapján sor kerülhet.

17.2 Ha a Közös Munkacsoport máshogy nem dönt, a DNS- és ujjnyomat-adatok automatizált keresésének és összehasonlításának feltételeit hat hónappal az ezen Végrehajtási megállapodás alapján folytatott tevékenységek megkezdését követően kell értékelni. A gépjármű-nyilvántartási adatok tekintetében az értékelésre három hónappal a tevékenységek megkezdése után kerül sor. Ezt követően a Szerződés 43. Cikke szerint bármely Fél kezdeményezheti ezeket az értékeléseket.

17.3 A Szerződés 39. Cikk (2) bekezdése értelmében a rögzítésért felelős szervek a Szerződés 3., 9. és 12. Cikkében előírt, az egyes külföldi kapcsolattartó pontok által végzett automatizált keresések jogszerűségének hatékony ellenőrzését biztosító mértékben és gyakorisággal szúrópróbaszerű ellenőrzéseket végezhetnek.

18. Az automatizált adatcsere rendelkezésre állása

A Felek minden ésszerű erőfeszítést megtesznek azért, hogy a DNS-, ujjnyomat- és gépjármű-nyilvántarási adatok automatizált, online cseréje a hét minden napján napi 24 órában rendelkezésre álljon. Műszaki hiba esetén a Felek megfelelő kapcsolattartó pontjai a lehető leghamarabb tájékoztatják egymást, és megegyeznek a bármilyen más jogi eszköz alapján ideiglenesen használandó alternatív kommunikációs csatornáról. Az automatizált adatcserét a lehető leghamarabb helyre kell állítani.

19. A Végrehajtási megállapodás és Mellékleteinek módosítása

19.1 Ezen Végrehajtási megállapodás és Mellékleteinek módosítását bármely Fél javasolhatja. Ezt a javaslatot az összes többi Fél részére el kell juttatni.

19.2 Ha a javasolt módosítás a Végrehajtási megállapodás rendelkezéseivel kapcsolatos, a Szerződés 43. Cikk (1) bekezdése szerinti Miniszterek Bizottsága dönt elfogadásáról.

19.3 Ha a javasolt módosítás a Végrehajtási megállapodás egy vagy több Mellékletével kapcsolatos, a Szerződés 43. Cikk (2) bekezdése szerinti Miniszterek Bizottsága dönt elfogadásáról.

19.4 A Végrehajtási megállapodás vagy Mellékleteinek módosításához az egyhangúságot akkor érik el, ha a részt vevő és képviselt Felek egyetértenek a javasolt módosítással. Ebből adódóan a hiányzó és nem képviselt Felek nem akadályozzák meg a Végrehajtási megállapodás módosításának elfogadását. A módosítás minden Felet köt.

20. Hatálybalépés, aláírás, letéteményes

20.1 Azon Felek estében, amelyeknél a Szerződés hatályba lépett, a Végrehajtási megállapodás aláírása, valamint a Szerződés 34. Cikk (2) bekezdésében előírt szükséges határozat meghozatala után lép hatályba. A többi Fél számára a Szerződés 50. Cikk (1) bekezdésének illetve az 51. Cikk (1) bekezdésének megfelelően és a Szerződés 34. Cikk (2) bekezdésében előírt szükséges határozat meghozatala után lép hatályba.

20.2 Ezt a Végrehajtási megállapodást és mellékleteit német, spanyol, francia és holland nyelven írják alá, mind a négy szöveg egyenértékű.

20.3 Ezen Végrehajtási megállapodás és Mellékletei letéteményese a Németországi Szövetségi Köztársaság kormánya.

Brüsszel, 2006. december 5.

(Aláírások)

Mellékletek listája

A Mellékletek:	***DNS-profilok automatizált keresése***
A.1 Melléklet	DNS-vonatkozású bűnügyi technikai kérdések, egyezési szabályok és algoritmusok [FIMA]
A.2 Melléklet	Félkódszám-táblázat [PCNT]
A.3 Melléklet	Funkcionális feldolgozási és munkafolyamat-elemzés [FPWA]
A.4 Melléklet	DNS Interfész-ellenőrzési dokumentum [DICD]
A.5 Melléklet	Alkalmazási, biztonsági és kommunikációs architektúra [ASCA]

B Mellékletek:	***Ujjnyomat-adatok automatizált keresése***
B.1 Melléklet	Interfész-ellenőrzési dokumentum (ICD)
B.2 Melléklet	Ellenőrzésre elfogadott jelöltek maximum száma
B.3 Melléklet	Azonosított személyek ujjnyomat-adatainak napi maximum keresési kapacitásai
B.4 Melléklet	Azonosított személyek ujjnyomat-nyomainak napi maximum keresési kapacitásai

C Mellékletek:	***Gépjármű-nyilvántartási adatok automatizált keresése***
C.1 Melléklet	Gépjármű-nyilvántartási adatok automatizált keresésének közös adatkészlete
C.2 Melléklet	Adatbiztonság
C.3 Melléklet	Az adatcsere műszaki feltételei
C.4 Melléklet	A beérkező kéréseket feldolgozó kapcsolattartó pontok listája

D Mellékletek:	***Rendőri együttműködés***
D.1 Melléklet	A közös műveletek elindításának folyamata és a kapcsolattartó pontok (24. Cikk)
D.2 Melléklet	A határon átnyúló együttműködés során közvetlen veszély esetén haladéktalanul értesítendő hatóságok és az ebben a Mellékletben felsorolt elérhetőségekben bekövetkezett változások bejelentését szolgáló kapcsolattartó pontok (25. Cikk)
D.3 Melléklet	A Szerződés 28. Cikk (1) bekezdés harmadik mondata alapján szállítani tilos fegyverek, lőszerek és felszerelés, a Szerződés 28. Cikk (2) bekezdés alapján használni tilos fegyverek, lőszerek és felszerelés, illetve a jogi feltételek, a Szerződés 28. Cikk (5) bekezdés szerinti gyakorlati feltételek.

A Mellékletek

DNS-profilok automatizált keresése

A.1 Melléklet

DNS-vonatkozású bűnügyi technikai kérdések, egyezési szabályok és algoritmusok

Bevezetés

Ez a dokumentum tartalmazza a Szerződés értelmében kicserélendő DNS-profilokra vonatkozó követelményeket, valamint az egyezési és jelentési szabályokat. A kicserélhetőség növelésére létező (európai és Interpol-) szabványokat alkalmazunk.

DNS-profilok tulajdonságai

A DNS-profil 24 számpárból áll, amelyek az Interpol DNS-vizsgálataiban is használt 24 lókusz alléljait jelölik. Ezen 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 sor 7 szürke színnel jelzett lókuszát Európai Standard Lókuszkészletnek (*European Standard Set of Loci* – ESS/ISSOL) nevezik. A Felek által keresésre és összehasonlításra rendelkezésre bocsátott DNS-profiloknak, valamint a keresésre és összehasonlításra kiküldött DNS-profiloknak a 7 lókusz közül legalább 6-ot kell tartalmazniuk, és tartalmazhatják a többi 17 lókuszt vagy az üres helyeket, amennyiben ezek rendelkezésre állnak. Az egyezések pontosságának növelése érdekében ajánlatos minden rendelkezésre álló allélt az indexált DNS-profil adatállományban tárolni.

A vegyes profilok és a nem teljes lókuszok nem megengedettek, tehát minden lókusz allélértéke csak 2 számból áll, amelyek azonosak is lehetnek, ha az adott lókusz homozigóta.

A helyettesítő karaktereket és a mikrovariánsokat az alábbi szabályok szerint kell kezelni:

- A profilban bármely nem-numerikus érték (pl. . „o”, „f”, „r”, „na”, „nr” vagy „un”) automatikusan helyettesítő karakterré alakítandó, és minden keresésre egyezést mutat.

- A profilban csak a „0” „1” és „99” számértékek alakítandók át automatikusan helyettesítő karakterré, és mutatnak minden keresésre egyezést.
- Ha egy lókuszon 3 allél van, az első allélt fogadják el, a másik két allél „R”-ré (helyettesítő karakter”) alakítandó, és minden keresésre egyezést mutat.
- Ha az első vagy a második allélre helyettesítő érték utal, akkor a lókuszra adott számérték mindkét permutációja keresendő (pl. 12,R egyezik 12,14-gyel és 9,12-vel is).
- A pentanukleotid (Penta D, Penta E & CD4) mikrovariánsok az alábbiak szerint egyeztetendők:
  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 (az Interpol-adatbázis többi lókusza tetranukleotid) mikro-variánsok az alábbiak szerint egyeztetendők:
  x.1 = x, x.1, x.2
  x.2 = x.1, x.2, x.3
  x.3 = x.2, x.3, x+1

Egyezési szabályok

2 DNS-profil összehasonlítása azon lókuszok alapján végzendő, amelyekre egy allélpár-érték mindkét DNS-profilban rendelkezésre áll. Mindkét DNS-profilban az ESS/ISSOL legalább 6 lókuszának rendelkezésre kell állnia, az amelogeninen kívül.

Teljes egyezés alatt az az egyezés értendő, amikor a kérelmező és a megkeresett DNS-profiljában egyaránt szereplő, összehasonlított lókuszok minden allélértéke ugyanaz. Majdnem egyezés alatt az az egyezés értendő, amikor a 2 DNS-profilban összehasonlított allélok közül csak egy különbözik. A majdnem egyezés csak akkor fogadható el, ha a 2 összehasonlított DNS-profilban legalább 6 teljesen egyező lókusz van. A majdnem egyezés oka lehet:

- Ember által elkövetett gépelési hiba valamely DNS-profil keresési kérelembe vagy a DNS-adatbázisba történő bevitelekor, vagy
- egy allél-meghatározási vagy allél-lekérdezési hiba a DNS-profilképzési eljárás során.

Jelentési szabályok

A teljes és a majdnem egyezések is jelentendők.

Az egyezési jelentés a kérelmező nemzeti kapcsolattartó pontnak küldendő, és a megkeresett nemzeti kapcsolattartó pont számára is hozzáférhetővé kell tenni (hogy megbecsülhesse a találatnak megfeleltetett DNS-profillal kapcsolatos ügyre és/vagy személyes adatokra vonatkozó lehetséges további kérések fajtáját és számát).

A.2 Melléklet

Félkódszám-táblázat

A Szerződés keretei közt a zárt hálózaton keresztüli prümi DNS-adatcsere-alkalmazásokban előírt doménnevek és más konfigurációs paraméterek létrehozásához az ISO 3166-1 alpha-2 kód használatáról döntöttek.

Az ISO 3166-1 alpha-2 kódok kétbetűs Félkódok. Az ISO 3166-1 szabvány legjobban ismert részeit képezik és – néhány változtatással – az internetes doménneveknél is ezeket használják.

Fél megnevezése	Kód
Belgium	BE
Németország	DE
Spanyolország	ES
Franciaország	FR
Luxemburg	LU
Hollandia	NL
Ausztria	AT

A.3 Melléklet

Funkcionális feldolgozási és munkafolyamat-elemzés

1. MUNKAFOLYAMAT

Ez a fejezet tartalmazza a minden Fél adatbázisának automatizált keresési és összehasonlítási eljárásai során alkalmazott munkafolyamat (az úgynevezett prümi konzultáció) leírását, a Végrehajtási megállapodás 4.3. és 4.4. pontjával összhangban.

1.1 Adatátadási eljárás a Szerződés 3. Cikke szerint:

1.1.1 Azonosítatlan DNS-profil

- TALÁLAT a nemzeti adatbázisban egy referencia DNS-profil kapcsán – nincs átadás.
- TALÁLAT a nemzeti adatbázisban egy másik azonosítatlan DNS-profillal – nincs átadás. Az összehasonlítás a Szerződés 4. Cikkében rögzített eljárás szerint történik.
- NINCS TALÁLAT a nemzeti adatbázisban – átadás minden adatbázis számára, ha a Fél nemzeti joga ezt lehetővé teszi:
  - TALÁLAT referencia DNS-profil kapcsán: automatizált értesítés a TALÁLATRÓL, és a profil(ok) értéke(i)nek átadása

- TALÁLAT egy azonosítatlan DNS-profil kapcsán: automatizált értesítés a TALÁLATRÓL, és a profil(ok) értéke(i)nek átadása.
- Megjegyzést lehet hozzáfűzni minden nemzeti adatbázisban, ahol TALÁLAT volt – a konzultációs eljárás megkezdése.
- NINCS TALÁLAT: automatizált NINCS TALÁLAT értesítés.

1.1.2 Referencia DNS-profil

- TALÁLAT a nemzeti adatbázisban egy referencia DNS-profil kapcsán – nincs átadás.
- TALÁLAT a nemzeti adatbázisban egy másik azonosítatlan DNS-profillal – nem kell átadás, ha egy megjegyzést hozzáfűznek.
- TALÁLAT a nemzeti adatbázisban egy megjegyzéssel ellátott azonosítatlan DNS-profillal – TALÁLAT külföldön: a konzultációs eljárás második szakasza
- NINCS TALÁLAT a nemzeti adatbázisban – átadás minden adatbázis számára, ha a Fél nemzeti joga ezt lehetővé teszi:
  - TALÁLAT referencia DNS-profil kapcsán: automatizált értesítés a TALÁLATRÓL, és a profil(ok) értéke(i)nek átadása
  - TALÁLAT egy azonosítatlan DNS-profil kapcsán: automatizált értesítés a TALÁLATRÓL, és a profil(ok) értéke(i)nek átadása.
  - Megjegyzést lehet hozzáfűzni minden nemzeti adatbázisban, ahol TALÁLAT volt – a konzultációs eljárás megkezdése.
  - NINCS TALÁLAT: automatizált NINCS TALÁLAT értesítés.

1.2 A Szerződés 4. Cikke szerinti adatátadási eljárás:

Első lépésként, amennyiben a Felek nemzeti joga ezt lehetővé teszi, a bűntettek helyszínén rögzített minden azonosítatlan DNS-profilra rákeresnek a Felek teljes adatállományában. Az ellenőrzési célú tömeges keresés a későbbiekben lehetséges.

- A kezdeti összehasonlítást el kell végezni az azonosítatlan DNS-profilokkal.
- Az alábbi esetek fordulhatnak elő:
  - Amennyiben a külföldi adatbázisban TALÁLAT van a referencia DNS-profil kapcsán: automatizált értesítés a TALÁLATRÓL, és a profil(ok) értéke(i)nek átadása – a konzultációs eljárás második lépése – mindegyik Fél eldöntheti, hogy tegyen-e megjegyzést az adatbázisban. A Felek kezdeményezésére külön megjegyzést lehet tenni az adatbázisban, ha egy azonosítatlan DNS-profil kapcsán találat volt egy nemzeti DNS-adatbázis és egy másik Fél DNS-adatbázisa közt.
  - Amennyiben a külföldi adatbázisban NINCS TALÁLAT: mivel a Szerződés lehetővé teszi a rendszeres összehasonlítást, minden Fél eldöntheti, hogy milyen (mértékű és gyakoriságú) vizsgálatot alkalmaz a 4. Cikkben előírt összehasonlítás során.
- Ha a nemzeti adatbázisok több azonos, különböző bűncselekményekből származó profilt tartalmaznak, a kérelmező Fél ezek közül csak egyet bocsát egyezőségi vizsgálatra, hogy elkerülje a munka fölösleges megsokszorozását.
- A szerződés 4. Cikkében meghatározott egyezőségi vizsgálat további részleteiről a kompetens hatóságoknak kétoldalúan kell megállapodniuk.

2. FUNKCIONÁLIS ELEMZÉS: ELSŐ LÉPÉS

2.1 A Szerződés 2. Cikk (3) bekezdése alapján tett nyilatkozatok:

AUSZTRIA: Ausztria kizárólag az európai elfogatóparancsról és a tagállamok közti átadási eljárásokról szóló 2002. június 13-i tanácsi kerethatározat (Hivatalos Lap, No. L 190, 2002. július 18., 1) 2. Cikk (1) illetve (2) bekezdésében az európai elfogatóparancs kiadásához előírt előfeltételeket teljesítő bűncselekmények üldözésének céljára teszi lehetővé a többi Fél nemzeti kapcsolattartó pontja számára, hogy hozzáférjenek a DNS-elemzési fájljaiban tárolt DNS-referenciaadatokhoz, a DNS-profilok összehasonlításával végzett automatizált keresésekhez való jogkörrel.

BELGIUM: Belgium csak az elítélt bűnelkövetők DNS-adatbázisát teszi hozzáférhetővé a többi Fél számára.

NÉMETORSZÁG: A Szerződés 2. Cikk (3) bekezdése alapján annak 2.-6. Cikkei a Német Szövetségi Köztársaság nemzeti DNS-elemzési adatbázisaira alkalmazandók, amelyeket kombinált alkalmazásként a Szövetségi Bűnügyi Rendőrség a Szövetségi Bűnügyi Rendőrségről szóló törvény 2., 7. és 8. szakasza értelmében, a szövetségi kormány és a tartományok közti bűnügyi együttműködés keretei közt tart fenn. A DNS-elemzési adatbázis a bűntett helyszínén rögzített anyagmaradványokat társítja az ismert bűnelkövetőkkel, a bűncselekményekben való nyomozások céljából. A Szerződés keretei közti adategyeztetés céljából csak a Szerződés 2. Cikk (2) bekezdésének 2. mondata szerinti referencia-adatot bocsátják rendelkezésre. Ez tehát a DNS-elemzési adatbázisokban tárolt adatok egy alkészlete.

SPANYOLORSZÁG: A Szerződés 2. cikk (3) bekezdésével összhangban a Szerződés 2–6. Cikkei a spanyol belügyminisztérium biztonsági államtitkára által felügyelt INT-SAIP adatbázisra alkalmazandók. Ennek az adatbázisnak a célja az igazságügyi szervek támogatása a nyomozásokban, a biológiai anyagmaradványok genetikai azonosítása és az ismert forrásból származó minták azonosítása révén. Ez az adatbázis tárolja a bűncselekményekre, az azonosításra és a személyes adatokra vonatkozó információkat. A Szerződés 2. Cikk (2) bekezdése alapján azonban a többi Fél számára csak azokat a referencia-adatokat teszik hozzáférhetővé, amelyekből az adatalanyt nem lehet közvetlenül azonosítani.

FRANCIAORSZÁG: Az adatbázisba való betekintés nem lehetséges kisebb súlyú bűncselekmények esetén.

HOLLANDIA: Hollandia biztosítja a nemzeti DNS-adatbázisához a hozzáférést gyanúsítottak, elítélt elkövetők, elhalálozott áldozatok és megoldatlan bűncselekményekből származó biológiai anyagmaradványok tekintetében.

LUXEMBURG: A Szerződéssel összhangban álló automatizált DNS-keresés és összehasonlítás céljából Luxemburg hozzáférést biztosít a többi Fél nemzeti kapcsolattartó pontja számára a 2006. augusztus 25-i, a bűncselekményekkel összefüggő DNS-profilalkotásról szóló törvényben előírt két DNS-adatbázisához: a bűnügyi DNS-adatbázishoz (melynek részei többek között az azonosítatlan DNS-profilok és a folyamatban lévő bűnügyi nyomozásokban érintett gyanúsítottak DNS-profiljai) és az elítélt bűnelkövetők DNS-adatbázisához.

2.2 Konzultációk volumene/száma

A Szerződés hatékony végrehajtása érdekében minden Félnek készen kell állnia a beérkező kérések fogadására.

Ezért minden Fél megbecsülte, hogy saját rendszerének hány kérelmet kell majd megválaszolnia és hányszor kíván betekinteni más Felek adatbázisába.

Betekintések becsült mennyisége / év	**AT**	**BE**	**FR**	**DE**	**LU**	**NL**	**ES**
Azonosítatlan DNS-profilok	6 000	2 000	5 000	30 000	500	6 000	6 000
Referencia DNS-profilok	12 000	5 000	100 000	45 000	500	12 000	/

2.3 A rendszer rendelkezésre állása

A lekérdezések a beérkezés időrendi sorrendjében kell, hogy elérjék a megcélzott adatbázist, a válasznak pedig a kérelmező Félhez a lekérdezés beérkezését követően 15 perccel kell megérkeznie.

3. FUNKCIONÁLIS ELEMZÉS : MÁSODIK LÉPÉS

Ha egy Fél pozitív választ kap, a DNS-szakértő elvégzi a lekérdezésben átadott profil és a válaszként átadandó profil(ok) értékei közti összehasonlítást. A szakértő tanúsítja és ellenőrzi a profil bizonyító erejét.

A jogsegély-eljárások azt követően indulnak, hogy az automatizált betekintési fázisban „teljes egyezést” vagy a „majdnem egyezést” mutatnak ki, és a két profil közti egyezést jóváhagyják.

A.4 Melléklet

DNS Interfész-ellenőrzési dokumentum (ICD)

1. Bevezetés

1.1 Célkitűzések

Ezen Melléklet célja, hogy meghatározza a Felek DNS-adatbázisrendszerei közti DNS-profil információk cseréjére vonatkozó követelményeket. A fejléceket kifejezetten a prümi DNS-adatcsere

céljára definiálták, míg az adatrész az Interpol DNS-csere rendszer által használt XML-séma DNS-profil adatrészén alapul.

A megállapodás szerint az adatcsere SMTP-n (*Simple Mail Transfer Protocol*) keresztül történik, az internet-szolgáltató által rendelkezésre bocsátott központi relé levelező szerver használatával.

1.2 Cél

Ez az ICD csak az üzenet (e-mail) tartalmát határozza meg. Minden hálózat-specifikus és üzenet-specifikus kérdést egységesen kell definiálni, hogy a DNS-adatcsere műszaki alapjai közösek legyenek.

A közös definíciók közt legalább az alábbiakat kell meghatározni:

- Az üzenet tárgyának formátuma, az üzenet automatizált feldolgozhatóságának érdekében,
- hogy szükséges-e a tartalom rejtjelezése, és ha igen, milyen eljárásokat válasszanak erre,
- az üzenetek maximális hossza.

1.3 XML-struktúra és -alapelvek

Az XML-üzenet az alábbi strukturális elemekből áll:
- Fejléc, amely az átadásról tartalmaz információkat és
- adatrész, amely profil-specifikus információkat és magát a profilt tartalmazza.

Ugyanez az XML-séma használható kell, hogy legyen a kérés és a válasz során is. Az azonosítatlan DNS-profilok (4. Cikk) teljes ellenőrzésének céljára lehetővé kell tenni több profil egy üzenetben való megküldését. Meg kell határozni az egy üzenetben továbbítható profilok maximális számát. Ez a szám az üzenet megengedett maximális méretétől függ, és a levelezőszerver kiválasztása után kell meghatározni.

Példa XML-re:

```
<?version="1.0" standalone="yes"?>
<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <fejléc>
            (…)
      </fejléc>
      <adatok>
            (…)
</adatok>
      [<adatok>                    az adatstruktúra ismétlendő, ha egy SMTP-üzenetben
        (….)                       több profilt küldenek, ez csak a 4. Cikk szerinti esetekben lehetséges
      </adatok>   ]
</PRUEMDNAx
```

2. Az XML-struktúra definíciói

Az alábbi definíciók dokumentációs célokat és a jobb olvashatóságot szolgálják, a tényleges, kötelező információt egy XML-sémafájl (PRUEM DNA.xsd) tartalmazza.

2.1 A PRUEMDNAx séma

Az alábbi mezőket tartalmazza:

Mező	**Típus**	**Leírás**
Header	PRUEM_header	1-szer fordul elő
datas	PRUEM_datas	1 … 500-szor fordulhat elő

2.2 A fejléc-struktúra tartalma

2.2.1 PRUEM_header

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

Mező	**Típus**	**Leírás**
type	PRUEM_header_type	Az XML fájl
direction	PRUEM_header_dir	Az üzenet küldésének iránya
Ref	String	Az XML fájl referenciája
Generator	String	Az XML fájl generátora
schema_version	String	A használandó séma verziószáma
Requesting	PRUEM_header_info	Információ a kérelmező Félről
Requested	PRUEM_header_info	Információ a megkeresett Félről

2.2.2 PRUEM_header_type

Az üzenetben lévő adat típusa, értéke lehet:

Érték	Leírás
M	Több profil (4. Cikk)
S	Egy profil (3. Cikk)

2.2.3 PRUEM_header_dir

Az üzenetben lévő adat típusa, értéke lehet:

Érték	Leírás
R	Kérés
A	Válasz

2.2.4 PRUEM_header_info

A Felet és az üzenet dátumát/időpontját leíró struktúra. Az alábbi mezőket tartalmazza:

Mező	**Típus**	**Leírás**
Source_ISOCODE	string	A Fél ISO 3166-2 kódja
Destination_ISOCODE	String	
REQUEST_ID	String	Kérelem egyedi azonosítója
date	date	Üzenet létrehozásának dátuma
time	Time	Üzenet létrehozásának időpontja

2.3 A PRUEM Profile adatok tartalma

2.3.1 PRUEM_datas

Ez az XML-profil adatrészét leíró struktúra. Az alábbi mezőket tartalmazza:

Mezők	**Típus**	**Leírás**
date	Date	Profil tárolásának dátuma
type	PRUEM_datas_type	Profil típusa
result	PRUEM_datas_result	Lekérdezés eredménye
agency	String	A profilért felelős megfelelő szervezeti egység neve
PROFILE_IDENT	String	Egyedi Fél-profil azonosító
Message	String	Hibaüzenet, ha az eredmény = E
Profile	IPSG_DNA_profile	Ha az irány = A (Válasz) ÉS az eredmény ≠ H (Találat) üres
MATCH_ID	String	TALÁLAT esetén a kérelmező profil PROFILE-ID-je
QUALITY	PRUEM_hitquality_type	Találat jellemzője
HITCOUNT	Integer	Egyező allélok száma

PRUEM_hitquality_type

Érték	Leírás
0	Az eredeti kérelmező profilra hivatkozva: “Nincs Találat” esetén: csak visszaküldött eredeti kérelmező profil; “Találat” esetén: eredeti kérelmező, a Végrehajtási Megállapodás 4.3.7 és 4.4 pontjával összhangban.
1	Egyezés minden rendelkezésre álló alléllel, helyettesítő karakterek nélkül
2	Egyezés minden rendelkezésre álló alléllel, helyettesítő karakterekkel
3	Találat eltéréssel (Mikrovariáns)
4	Találat nem-egyezéssel

2.3.2 PRUEM_data_type

Az üzenetben lévő adat típusa, értéke lehet:

Érték	Leírás
P	Személyes profil
S	Nyom

2.3.3 PRUEM_data_result

Az üzenetben lévő adat típusa, értéke lehet:

Érték	Leírás
U	Nem meghatározott, ha az irány = R (kérelem)
H	Találat
N	Nincs találat
E	Hiba

2.3.4 IPSG_DNA_profile

DNS-profilt leíró struktúra. Az alábbi mezőket tartalmazza:

Mező	**Típus**	**Leírás**
ESS_ISSOL	IPSG_DNA_ISSOL	Az ISSOL (az Interpol standard lókuszcsoportja)-nak megfelelő lókuszcsoport
additional_loci	IPSG_DNA_additional_loci	Egyéb lókuszok
Marker	String	A DNS generálására használt módszer
profile_id	String	A DNS-profil egyedi azonosítója

2.3.5 IPSG_DNA_ISSOL

Az ISSOL (az Interpol standard lókuszcsoportja) lókuszait tartalmazó struktúra. Az alábbi meőket tartalmazza:

Mező	**Típus**	**Leírás**
Vwa	IPSG_DNA_locus	Vwa lókusz
th01	IPSG_DNA_locus	th01 lókusz
D21s11	IPSG_DNA_locus	d21s11 lókusz
Fga	IPSG_DNA_locus	fga lókusz
d8s1179	IPSG_DNA_locus	d8s1179 lókusz
d3s1358	IPSG_DNA_locus	d3s1358 lókusz
d18s51	IPSG_DNA_locus	d18s51 lókusz
Amelogenin	IPSG_DNA_locus	Amelogin lókusz

2.3.6 IPSG_DNA_additional_loci

Az egyéb lókuszokat tartalmazó struktúra. Az alábbi mezőket tartalmazza:

Mező	Típus	Leírás
Tpox	IPSG_DNA_locus	Tpox lókusz
csf1po	IPSG_DNA_locus	csf1po lókusz
d13s317	IPSG_DNA_locus	d13s317 lókusz
d7s820	IPSG_DNA_locus	d7s820 lókusz
d5s818	IPSG_DNA_locus	d5s818 lókusz
d16s539	IPSG_DNA_locus	d16s539 lókusz
d2s1338	IPSG_DNA_locus	d2s1338 lókusz
d19s433	IPSG_DNA_locus	d19s433 lókusz
penta_d	IPSG_DNA_locus	penta_d lókusz
penta_e	IPSG_DNA_locus	penta_e lókusz
Fes	IPSG_DNA_locus	fes lókusz
f13a1	IPSG_DNA_locus	f13a1 lókusz
f13b	IPSG_DNA_locus	f13b lókusz
se33	IPSG_DNA_locus	se33 lókusz
cd4	IPSG_DNA_locus	cd4 lókusz
Gaba	IPSG_DNA_locus	gaba lókusz

2.3.7 IPSG_DNA_locus

Lókuszt leíró struktúra. Az alábbi mezőket tartalmazza:

Mező	Típus	Leírás
low_allele	String	Egy allél legalacsonyabb értéke
high_allele	String	Egy allél legmagasabb értéke

A.5 Melléklet

Alkalmazási, biztonsági és kommunikációs architektúra

1. Áttekintés

A Szerződés keretei közti DNS-adatcserét elősegítő alkalmazások megvalósítása kapcsán arról döntöttek, hogy egy közös kommunikációs hálózatot alkalmaznak, amely a Felek közt logikailag zárt lesz. Azért, hogy a kérelmek küldése és a válaszok fogadása során hatékonyabban használják ki ezt a közös kommunikációs infrastruktúrát, a DNS- és az ujjnyomat-adat iránti kérelmek kódolt SMTP e-mailüzenetben történő továbbítására egy aszinkron mechanizmust hagytak jóvá. A biztonsági követelmények teljesítése érdekében – az SMTP-funkcionalitás kiterjesztéseként – az sMIME mechanizmust fogják alkalmazni a hálózat végpontjai közti csatorna biztonságának garantálására.

A működő TESTA II-t („Közigazgatásközi Transzeurópai Telematikai Szolgáltatások” – „***T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations*”) választották a Felek közti adatcsere kommunikációs hálózatának. A TESTA II-t jelenleg az Európai Bizottság működteti. Mivel a jelenlegi nemzeti DNS-adatbázisok illetve TESTA II-hozzáférési pontok egyes Feleknél esetleg eltérő helyen lehetnek, két lehetőség van a TESTA II-hozzáférés beszerzésére:

(1) a meglévő nemzeti hozzáférési pont használata, vagy új TESTA II hozzáférési pont létesítése, vagy
(2) egy biztonságos helyi kapcsolat kiépítése arról helyről, ahol a DNS-adatbázis található, és ahol az illetékes nemzeti hatóság azt kezeli, arra a helyre, ahol a meglévő nemzeti TESTA II hozzáférési pont van.

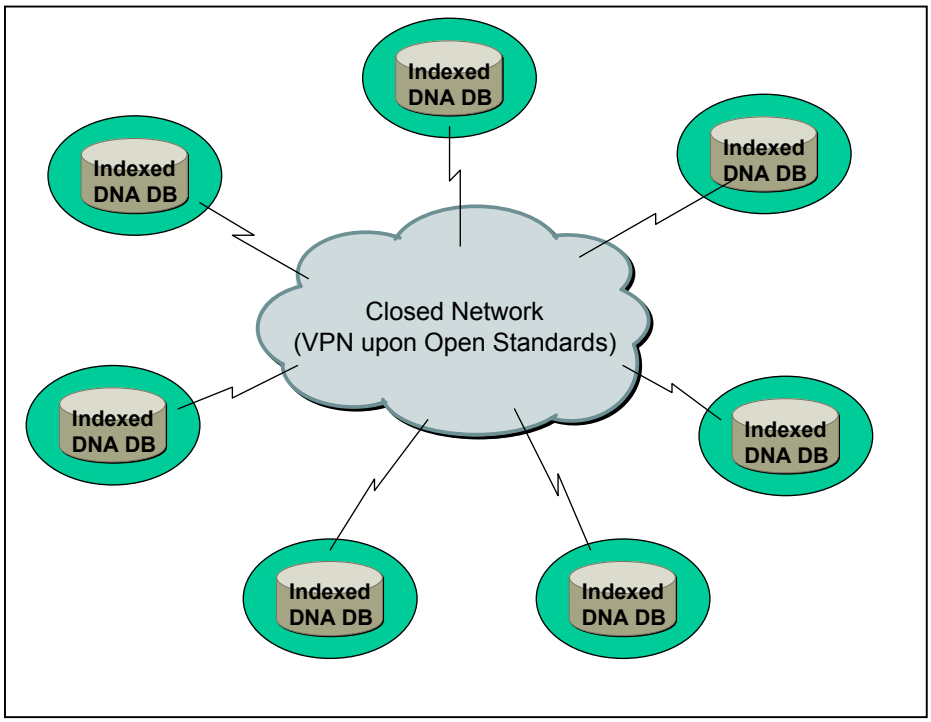
Mindegyik Fél maga döntheti el, hogy melyik lehetőséget választja. A hozzáférési sémát a Szerződéshez később csatlakozó államoknak is el kell fogadniuk.

A Szerződés alkalmazásainak megvalósítása során alkalmazott protokollok és szabványok megfelelnek a Nyílt Szabványoknak (*Open Standards*) és a Felek nemzeti biztonságpolitikai döntéshozói által támasztott követelményeknek.

2. Felső szintű architektúra

Minden Szerződő Fél hozzáférhetővé teszi rendelkezésére álló saját DNS-adatait a többi Féllel való csere és/vagy keresés céljára, a standardizált közös adatformátumnak megfelelően. A DNS-profilokat tároló központi számítógépes szerver nincs.

1. ábra: A DNS-adatcsere topológiája



A Felek telephelyein hatályos nemzeti jogi korlátozások figyelembe vételével minden Fél maga döntheti el, hogy milyen hardvert és szoftvert használ a szerződés előírásainak teljesítése érdekében.

3. Biztonsági szabályok és adatvédelem

A Szerződés szerinti DNS-adatcsere végrehajtása érdekében három biztonsági szintben egyeztek meg, és ezek alkalmazandóak.

3.1 Adatszint

A Felek által átadott DNS-profiladatot közös adatvédelmi szabályoknak megfelelően kell összeállítani, úgy, hogy a kérelmező Fél által megkapott válasz főként azt jelölje, hogy van-e találat vagy nincs; találat esetén egy olyan azonosító számmal, amely semmilyen személyes információt nem tartalmaz. A találatról szóló értesítést követően a további nyomozás bilaterális módon történik, az érintett Felek meglévő nemzeti jogi szabályozása és szervezeti sajátosságai szerint.

3.2 Kommunikációs szint

A (keresett és megválaszolt) DNS-profilinformációt tartalmazó üzeneteket egy, a nyílt szabványoknak megfelelő speciális mechanizmussal rejtjelezik mielőtt egy másik Fél részére elküldenék.

3.3 Átadási szint

Minden, DNS-profilinformációt tartalmazó rejtjelezett üzenet egy megbízott internet-szolgáltató által nemzetközi szinten adminisztrált virtuális privát csatornán és az ehhez a csatornához vezető, nemzeti felelősségi körbe tartozó, biztonságos kapcsolaton keresztül továbbítandó más Fél számára. Ennek a virtuális privát csatornának nincs kapcsolódási pontja a nyilvános internettel.

Ennek a három biztonsági szintnek a kihasználásával a Szerződés keretei közti DNS-adatcsere magas biztonsági követelményeknek tesz eleget. A háromszintű biztonsági architektúra használatával nagyban csökken annak veszélye, hogy az egész rendszer károsodjon ártó szándékú támadások következményeként.

4. A rejtjelezési mechanizmushoz használandó protokollok és standardok:

sMIME és kapcsolódó csomagok

A műszaki követelmények és a rendelkezésre álló technológiák figyelembe vételével az SMTP *de facto* e-mail-standard kiegészítéseként alkalmazott nyílt sMIME standard alkalmazandó a DNS-profilinformációt tartalmazó üzenetek rejtjelezésére. Az IETF s/MIME Munkacsoportja készíti jelenleg az s/MIME (V3)-at. Az s/MIME (V3) protokoll lehetőséget ad az aláírt bizonylatokra, biztonsági címkékre és biztonságos levelezési listákra, és a Cryptographic Message Syntax (CMS) – egy, rejtjelekkel védett IETF-specifikáció – alapján rétegezett. Használható digitális adatok bármilyen formájának digitális aláírására, feldolgozására, engedélyezésére vagy rejtjelezésére. Az sMIME mechanizmus által használt tanúsítvány meg kell, hogy feleljen az X.509 szabványnak.

Az s/MIME funkció a modern levelezőszoftver-csomagok túlnyomó többségébe – köztük az Outlook-ba, a Mozilla Mail-be és a Netscape Communicator 4.x–be – be van építve, és minden jelentősebb levelezőszoftver-csomag között működik.

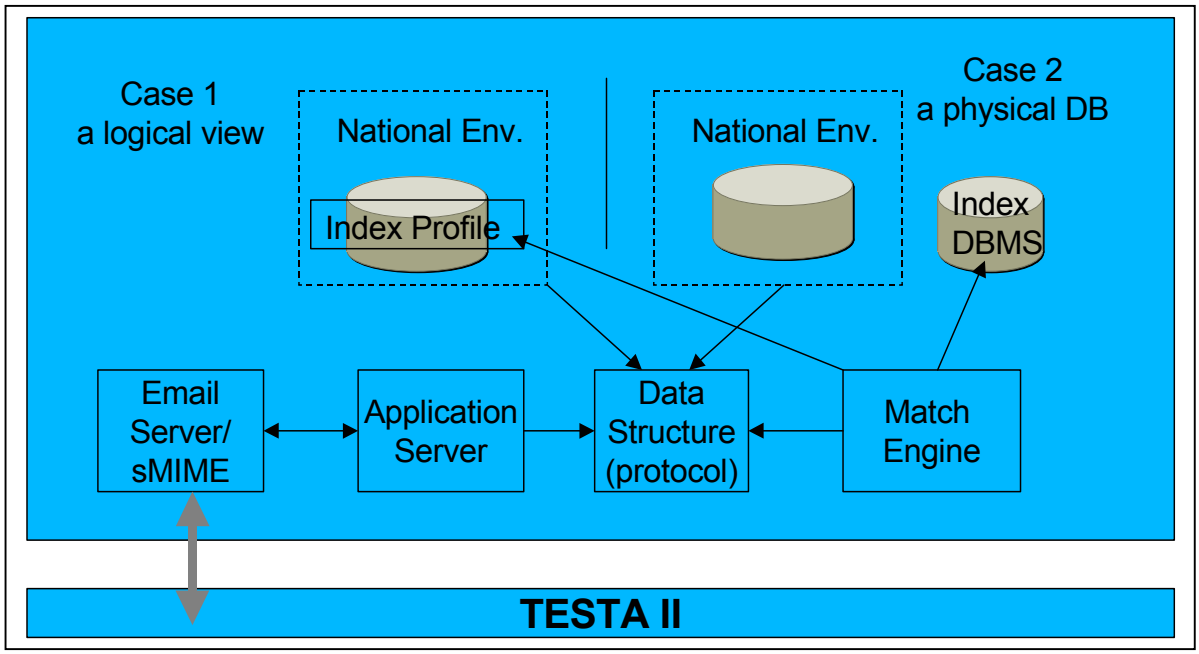
Azért esett az sMIMe-ra a választás, mert könnyen integrálható minden Fél nemzeti informatikai infrastruktúrájába és járható útja a kommunikáció biztonsági szintje megteremtésének. A DNS-adatcsere prototipizálására azonban a „*Proof of Concept*” cél hatékonyabb elérése és a költségek csökkentése érdekében a JavaMail API-t választották ki. A JavaMail API az s/MIME és/vagy az OpenPGP alkalmazásával rejtjelezi és fejti meg az e-maileket. A szándék az, hogy egyetlen, könnyen használható API-t biztosítsunk a levelezőknek, akik rejtjelezett e-maileket kívánnak küldeni vagy fogadni a két legnépszerűbb e-mail-rejtjelezési formátum egyikének alkalmazásával. Ezért a szerződés által előírt követelmények teljesítéséhez elegendő lesz a JavaMail API bármely egyedi alkalmazása. Az összes Fél közti DNS-adatcsere prototipizálására például a „*Bouncy Castle JCE*” (**J**ava ***C****ryptographic* ***E****xtension*) nevű terméket fogják használni.

5. Alkalmazási architektúra

A közös ICD alapján minden Fél standardizált DNS-profilkészletet ad át a többi Félnek. Két módja van a Szerződésnek megfelelő DNS-adat más Felek számára történő hozzáférhetővé tételének: logikai betekintés biztosítása az egyedi nemzeti adatbázisba, vagy egy fizikailag exportált adatbázis létrehozása. Ennek négy fő összetevője – e-mailszerver/sMIME; alkalmazásszerver; az adatok le- és feltöltésére, továbbá az érkező és elküldött üzenetek nyilvántartására szolgáló adatstruktúra-terület; valamint az egyezési program – termékfüggetlen módon hajtja végre a teljes alkalmazási logikát. Azért, hogy minden Fél könnyen integrálhassa az összetevőket saját nemzeti rendszerébe, ugyanazokat a funkciókat opcionális nyílt szabványok és protokollok alapján lehet végrehajtani, amelyeket minden Fél saját nemzeti informatikai politikájának és szabályozásának függvényében választhat meg. A Szerződésnek megfelelő DNS-profilokat tartalmazó indexált adatbázisokhoz való hozzáférés megszerzéséhez szükséges semleges elvek miatt minden Fél szabadon dönthet a hardver- és szoftverplatformról, beleértve az adatbázist és az operációs rendszereket.

Az önként jelentkező Felek szakértőiből álló csapat dolgozza ki a prototípust, azzal a céllal, hogy bebizonyítsák, a koncepció működik. A többi, nem prototipizáló Fél opcionálisan elfogadhatja ezt a prototípust, esetleg bizonyos mértékű testreszabással, de nem köteles ezt megtenni. A nem prototipizáló Felek saját terméket is kidolgozhatnak a Szerződés kommunikációs környezetéhez való csatlakozásra a jelen Végrehajtási megállapodás által előírt specifikációkkal összhangban.

2. ábra: Az alkalmazási topológia áttekintése



6. Az alkalmazási architektúrához használandó protokollok és standardok:

6.1 XML

A DNS-adatcsere az SMTP e-mail üzenetekhez mellékelt XML-sémát használja. Az e**X**tensible **M**arkup **L**anguage (**XML**) egy, a W3C által ajánlott általános célú leíró nyelv, mely speciális célú leíró nyelvek létrehozására használható, különböző adattípusok leírására képes. Az összes Fél közti cserére alkalmas DNS-profil leírását XML és XML-séma alapján készítették az ICD-dokumentumban.

6.2 ODBC

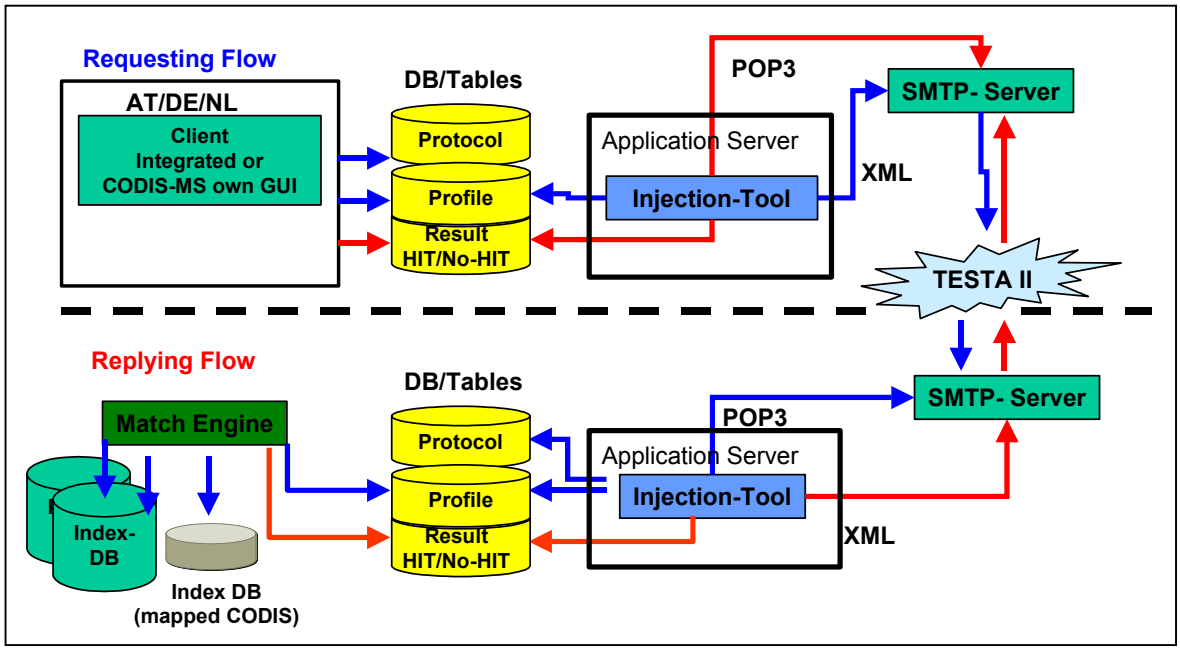
Az Open **D**ata**B**ase **C**onnectivity standard szoftveres API-módszert nyújt az adatbázis-kezelő rendszerekhez való hozzáféréshez, függetlenítve azt a programozási nyelvektől, adatbázisoktól és operációs rendszerektől. Az ODBC-nek azonban van néhány hátránya. Nagyszámú kliensgép kezelése többféle driver és DLL használatával járhat. Ez a komplexitás növelheti a rendszeradminisztráció időigényét.

6.3 JDBC

A Java **D**ata**B**ase **C**onnectivity (**JDBC**) a Java programnyelv egy API -ja, amely meghatározza, hogy egy kliens hogyan férhet hozzá az adatbázishoz. Az ODBC-vel ellentétben a JDBC nem követeli meg egy bizonyos helyi DLL-készlet használatát a munkaállomáson.

A DNS-profilok iránti kérések és a válaszok feldolgozásának folyamatát a Feleknél az alábbi ábra szemlélteti. A kérelmező és a válaszoló áramlatok is egy semleges adatterülettel vannak kölcsönhatásban, amely egy közös adatstruktúrával rendelkező különböző adatállományokból áll.

3. ábra: Az alkalmazási architektúra áttekintése a Feleknél



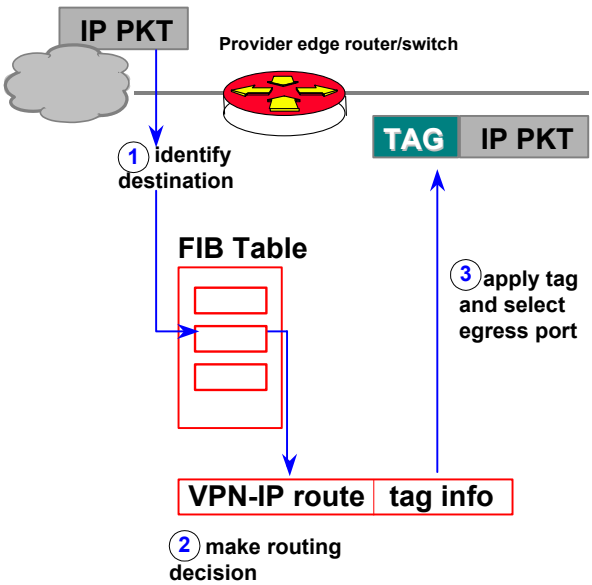
7. Kommunikációs környezet

7.1 Közös kommunikációs hálózat: a TESTA II és további infrastruktúrái

A DNS-adatcsere-alkalmazás az e-mailt mint aszinkron mechanizmust használja a Felek közti kérések küldésére és a válaszok fogadására. Mivel minden Félnek van legalább egy nemzeti hozzáférési pontja a TESTA II-höz, a DNS-adatcsere-műveletet a TESTA II hálózaton keresztül bonyolítják. A TESTA II számos hozzáadott értéket képviselő szolgáltatást nyújt, az e-mail-relén keresztül. A TESTA II-specifikus e-mail postafiókokon kívül a rendszer levélterjesztési listákat és routing-szabályokat is alkalmazni tud. Ezért a TESTA II az európai doménekhez kapcsolt közigazgatásoknak címzett üzenetek klíringházaként szolgálhat. Vírusellenőrzési mechanizmusok telepítésére is mód van. A TESTA II e-mail-relé a központi TESTA II-létesítményben található nagykapacitású hardverplatformra épül, és tűzfal által védett. A TESTA II **D**omain **N**ame **S**ervices (DNS) feloldja a forráslokátorokat az IP-címekre, és elrejti a felhasználók és az alkalmazások elől a címzéseket.

7.2 Biztonsági kérdések

A Virtuális Privát Hálózatot (*Virtual Private Network* – VPN) a TESTA II keretei közt hozták létre. Az ennek kiépítéséhez használt címkeváltási technológia (*Tag Switching Technology*) továbbfejlesztve az *Internet Engineering Task Force* (IETF) által fejlesztett *Multi-Protocol Label Switching* (MPLS) szabvánnyá fog válni.



Az MPLS egy IETF szabványtechnológia, amely felgyorsítja a hálózati adatáramlást a köztes routerek (*hops*) általi csomagelemzés elkerülésével. Ezt úgynevezett címkék segítségével teszi, amelyeket a gerinchálózat határrouterei tesznek a csomagokra a továbbító információs bázisban (FIB) tárolt információk alapján. A címkéket a VPN-ek alkalmazására is használják.

Az MPLS a 3-rétegű routing előnyeit a 2-rétegű kapcsoláséival kombinálja. Mivel az IP-címeket a gerincen keresztüli átvitel során nem ellenőrzik, az MPLS semmilyen IP-címzési korlátozást nem követel meg.

Ezen felül, a TESTA II-n keresztüli e-mailüzeneteket egy sMIME-vezérelt rejtjelezési mechanizmus védi. A kulcs és a megfelelő tanúsítvány birtoklása nélkül senki sem fejtheti meg az üzeneteket a hálózaton keresztül.

7.3 A kommunikációs hálózatban használandó protokollok és szabványok

7.3.1 SMTP

A **S**imple **M**ail **T**ransfer **P**rotocol az interneten keresztüli e-mailtovábbítás *de facto* szabványa. Az SMTP egy viszonylag egyszerű, szövegalapú protokoll, amelyben az üzenet egy vagy több címzettjét állapítják meg, majd az üzenet szövegét továbbítják. Az SMTP az IETF specifikációja alapján a 25-ös TCP-portot használja. Egy adott doménnév SMTP-szerverének meghatározásához az MX (*Mail eXchange*) DNS (*Domain Name Systems*)-adatot használják.

Mivel a protokoll kezdetben egyszerű ASCII -szöveg-alapú volt, nem tudta kezelni a bináris fájlokat. A MIME -hoz hasonló standardokat azért fejlesztették ki, hogy a bináris fájlokat az SMTP-s átvitelhez kódolják. Manapság a legtöbb SMTP-szerver támogatja a 8BITMIME és az sMIME-kiterjesztéseket, lehetővé téve a bináris fájloknak a sima szövegéhez közel hasonlóan könnyű átvitelét.

Az SMTP egy „*push*” protokoll, amely nem teszi lehetővé, hogy valaki egy távoli szerverről „lehúzza” (*pull*) az üzeneteket. Ehhez a levelezőkliensnek a POP3 -at vagy az IMAP-ot kell használnia. A DNS-adatcsere megvalósítására a POP3 protokoll használatáról született döntés.

7.3.2 POP

A helyi e-mail kliensek a **P**ost **O**ffice **P**rotocol **3**-as verzióját (**POP3**) használják, amely egy, távoli szervertől TCP/IP kapcsolaton keresztül történő e-maillletöltésre szolgáló alkalmazás-rétegű internetes protokoll. Az SMTP protokoll SMTP „Submit” profilját használva az e-mail kliensek az interneten vagy egy vállalati hálózaton keresztül küldik az üzeneteket. A MIME az e-mail mellékleteinek és nem ASCII szövegeinek standardjéül szolgál. Bár sem a POP3, sem az SMTP nem követeli meg a MIME-formátumú e-mailt, az internetes e-mail alapvetően MIME-formátumban érkezik, tehát a POP-klienseknek is érteniük és használniuk kell a MIME-ot. Ezért a Szerződés teljes kommunikációs környezete a POP elemeiből fog állni.

7.4 Hálózaticím-séma

Az európai IP-regisztrációs Hatóság (RIPE) a TESTA II-höz rendelte a 62.62.0.0/17-es címblokkot. A TESTA II-höz a jövőben további címblokkok rendelhetőek, ha erre szükség van (de csak ha a 62.62.0.0/17 legalább 80 százalékát már hozzárendelték a TESTA II hálózathoz, és ténylegesen használják). A TESTA II hálózathoz rendelt címtartomány a 62.62.0.0 – 62.62.127.255. A fent említett földrajzi megközelítésre tekintettel minden országhoz egy külön C-osztályú alhálózat-blokkot rendelnek.

A jelenlegi Felek számára a TESTA II vezetősége az alábbi táblázatban leírt IP-címtartományokat rendeli és/vagy foglalja le:

IP-címtartomány	Fél	Kommentár
62.62.0.0/24 – 62.62.1.0/24	Központi szolgálat (TESTA II)	
62.62.30.0/24 – 62.62.33.0/24	Ausztria	
62.62.22.0/24 – 62.62.25.0/24	Belgium	

IP-címtartomány	Fél	Kommentár
62.62.50.0/24	Franciaország	
62.62.38.0/24 to 62.62.40.0/24	Németország	első rész
62.62.76.0/24 to 62.62.79.0/24	Németország	második rész
62.62.54.0/24	Hollandia	
62.62.26.0/24 – 62.62.29.0/24	Luxemburg	
62.62.6.0/24 – 62.62.9.0/24	Spanyolország	

A TESTA II továbbfejlesztése során az IP-címtartományok változhatnak.

7.5 Konfigurációs paraméterek

Az **eu-admin.net** domént használva egy biztonságos e-mailrendszert hoznak létre. Ez a domén, a hozzá társított IP-címekkel együtt nem lesz hozzáférhető a TESTA II európai doménjén kívülről, mivel a nevek csak a TESTA II központi DNS-szerveren ismertek, amelyik az internetről nem látható.

Ezen TESTA II site-ok címeinek (host-ok neveinek) IP-cím feloldását a TESTA II DNS-szolgálata végzi. Minden helyi doménhez hozzáadnak egy levelezési belépést ehhez a TESTA II központi DNS-szerverhez, minden, a TESTA helyi doménekre érkező e-mailüzenetet továbbítva a TESTA II központi levelezőreléjére. Ez a TESTA II központi levelezőrelé ezt követően a helyi domén e-mailcímeket használva továbbítja azokat az adott helyi domén e-mailszerverére. Az e-mailek ilyen módon történő továbbítása révén a bennük található kritikus információ csak az európai zárt hálózati infrastruktúrán megy keresztül, nem pedig a nem biztonságos interneten.

Szükség van aldomének (***fékövér, dőlt betűk***) létrehozására minden Félnél, az alábbi szintaxist követve:
"***application-type*.pruem.*party-code*.**eu-admin.net", ahol:
"party-code" az alábbi értékek egyikét veszi fel: AT, BE, DE, ES, FR, LU vagy NL; a Félkód egy országkód;
"***application-type***" az alábbi értékek egyikét veszi fel: DNA vagy FP.

A fenti szintaxist követve a jelenlegi hét Fél aldoménjait az alábbi táblázat foglalja össze:

Tagállamok/Felek	Aldomének	Kommentár
Ausztria	***dna*.pruem.at**.eu-admin.net	A meglévő TESTA II nemzeti hozzáférési pontot használva.
	***fp*.pruem.at**.eu-admin.net	
Belgium	***dna*.pruem.be**.eu-admin.net	Biztonságos kapcsolat kiépítése a meglévő TESTA II hozzáférési ponthoz.
	***fp*.pruem.be**.eu-admin.net	
Németország	***dna*.pruem.de**.eu-admin.net	A meglévő TESTA II nemzeti hozzáférési pontot használva.
	***fp*.pruem.de**.eu-admin.net	
Spanyolország	***dna*.pruem.es**.eu-admin.net	A meglévő TESTA II nemzeti hozzáférési pontot használva.
	***fp*.pruem.es**.eu-admin.net	
Franciaország	***dna*.pruem.fr**.eu-admin.net	A meglévő TESTA II nemzeti hozzáférési pontot használva.
	***fp*.pruem.fr**.eu-admin.net	

Tagállamok/Felek	Aldomének	Kommentár
Luxemburg	***dna*.pruem.lu**.eu-admin.net	A meglévő TESTA II nemzeti hozzáférési pontot használva.
	***fp*.pruem.lu**.eu-admin.net	
Hollandia	***dna*.pruem.nl**.eu-admin.net	Megkísérelnek kiépíteni egy új TESTA II hozzáférési pontot az NFI-nél
	***fp*.pruem.nl**.eu-admin.net	

8. Következtetések

Az Európai Bizottsággal (COM) folytatandó tárgyalások eredménye alapján a DNS-alkalmazás TESTA II-n keresztüli használatának lépésenkénti megközelítését fogadják el. Bizonyos mértékű testreszabásra van szükség, főleg az Európai Bizottság (COM) által a TESTA II-szolgáltatóval együttműködésben. Azonban minden Fél maga felelős az IT-környezet és szükség esetén a site-ok módosításaiért. Az első TESTA II-n keresztüli alkalmazást a prototipizáló Felek között tervezik megvalósítani, míg a többi Fél a szükséges informatikai és szervezeti követelmények teljesülését követően készen kapná az alkalmazást. A nem-prototipizáló Feleknek az alkalmazás megkezdése előtt időben megküldik kitöltésre a követelmények listáját.

B Mellékletek

Ujjnyomat-adatok automatizált keresése

B.1 Melléklet

Interfész-ellenőrzési dokumentum (ujjnyomat-adatok)

Bevezetés

Ezen dokumentum célja, hogy meghatározza a Felek automatizált ujjnyomat-azonosítási rendszerei (AUAR) közti ujjnyomatinformáció-csere követelményeit. Alapjául az Interpol ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b) szolgál.

Ez a változat a kép- és sablon (*minutiae*)-alapú ujjnyomat-feldolgozáshoz szükséges 1., 2., 4., 9. és 13. és 15. típusú logikai rekordok minden alapmeghatározását lefedi.

1. A fájl tartalmának áttekintése

Egy ujjnyomat-fájl több logikai rekordból áll. Az eredeti ANSI/NIST-ITL 1-2000 szabványban 16 rekordtípust definiáltak. A megfelelő ASCII szeparációs karaktereket alkalmazzák a rekordok közt, illetve a rekordokon belül a mezők és almezők közt.

A Szerződés alkalmazásának ezen változatában csak 6 rekordtípust használnak a forrás- és a célszervezet közti információcserére.

1. típus -> Tranzakciós információ
2. típus -> Személyek/ügyek betű-szám adatai
4. típus -> Ujjnyomatok nagy felbontású szürkeskálás képei
9. típus -> Sablon (*minutiæ*)-rekord
13. típus -> Változó felbontású látens kép
15. típus -> Változó felbontású látens tenyérnyomat-kép rekord

1.1 1. típus – Fájl-fejléc

Ez a rekord routing–információkat, illetve a fájl többi részének struktúráját leíró információkat tartalmaz. Szintén ez a rekordtípus jelöli azt a tranzakciótípust, amely az alábbi tág kategóriák egyikébe sorolható:

1.2 2. típus – Leíró szöveg

Ez a rekord a küldő és a fogadó szervezet számára értékes szöveges információkat tartalmaz.

1.3 4. típus – Nagy felbontású szürkeskálás kép

Ezt a rekordot 500 pixel/inch-es, nagy felbontású szürkeskálás (nyolcbites) ujjnyomat-képek cseréjére használják. Az ujjnyomat-képeket a WSQ-algoritmus szerint kell tömöríteni, legfeljebb 1:15 arányban. Nem szabad más tömörítési eljárásokat, illetve tömörítetlen képeket használni.

1.4 9. típus – Sablon (Minutiæ)- rekord

A 9. típusú rekordokat a sablonadatok barázdaadataira használják. Céljuk egyrészt, hogy elkerüljék az AUAR-kódolási eljárások felesleges megsokszorozását, másrészt, hogy a megfelelő képeknél kevesebb adatot tartalmazó AUAR-kódok átadását lehetővé tegyék.

1.5 13. típus – Változó felbontású látens kép-rekord

Ezt a rekordot a változó felbontású látens ujj- és tenyérnyomatképek szöveges alfanumerikus információkkal együtt történő cseréjére használják. A képek szkennelt felbontása 500 pixel/inch kell, hogy legyen, a szürke szín 256 árnyalatával. Ha a látens kép minősége megfelelő, a WSQ-algoritmussal tömörítendő. Szükség esetén a képek felbontását – kétoldalú megállapodás alapján – 500 pixel/inch-nél, illetve 256 szürkeárnyalatnál magasabbra lehet növelni.

1.6 15. típus – Változó felbontású tenyérnyomatkép-rekord

A 15. típusú mezőcímkézett képrekordokat változó felbontású tenyérnyomatképek szöveges alfanumerikus információkkal együtt történő cseréjére használják A képek szkennelt felbontása 500 pixel/inch kell, hogy legyen, a szürke szín 256 árnyalatával. Az adatmennyiség minimalizálása érdekében minden tenyérnyomat-kép WSQ-algoritmussal tömörítendő. Szükség esetén a képek felbontását – kétoldalú megállapodás alapján – 500 pixel/inch-nél, illetve 256 szürkeárnyalatnál magasabbra lehet növelni.

2. Rekordformátum

Egy tranzakciós fájl egy vagy több logikai rekordból állhat. A fájl minden logikai rekordjánál meg kell lenniük a hozzá való információs mezőknek. Minden információs mező egy vagy több alapvető, egyértékű információs egységből állhat. Ezek az egységek együtt az adott mező adatainak különböző tulajdonságait továbbítják. Egy információs mező egy vagy több egybecsoportosított, és a mezőn belül többször megismételt egységből is állhat. Az információs egységek ezen csoportját almezőnek nevezik. Egy információs mező tehát információs egységek egy vagy több almezőjéből állhat.

2.1 Információ-szeparátorok

A mezőcímkézett logikai rekordokban az információk elhatárolása négy ASCII információ-szeparátor használatával történik. Az elhatárolt információk lehetnek egy mezőn vagy almezőn belüli egységek, egy logikai rekordon belüli mezők, vagy különböző almezők. Ezeket az információ-szeparátorokat az ANSI X3.4 szabvány definiálja. Ezek a karakterek az információk logikai úton való elválasztására és minősítésére szolgálnak. Hierarchikus szempontból a fájlszeparátor („FS”)-karakter a legátfogóbb, ezt követi a csoportszeparátor- („GS”), a rekordszeparátor- („RS”), és végül az egységszeparátor („US”)-karakter. Az 1. táblázat ezeket az ASCII-szeparátorokat, illetve a szabvány szerinti használatukat írja le.

Az információs szeparátorok funkcionális szempontból az őket követő adatok típusának jelzéseként foghatók fel. Az „US” karakter az egy mezőn vagy almezőn belüli egyedi információs egységeket választja el egymástól. Ez azt jelzi, hogy a következő információs egység az adott mezőhöz vagy almezőhöz tartozik. Egy „RS” karakterrel elválasztott mezőn belüli almezők, információs egység(ek) következő ismétlődő csoportjára utal. Az információs mezők közt használt „GS” szeparátor karakter egy olyan új mező kezdetét jelzi, amely a megjelenő mező-azonosítószámot megelőzi. Ehhez hasonlóan egy új logikai rekord kezdetét az „FS” karakter megjelenése jelzi.

A négy karakter csak akkor értelmes, ha az ASCII szövegrekordok mezőin belüli adategységek szeparátoraként használják őket. A bináris képrekordokban, illetve bináris mezőkben előforduló ezen karakterek nem hordoznak külön jelentést, egyszerűen a kicserélt adat részét képezik.

Általában nem fordulhatnak elő üres mezők vagy információs egységek, tehát bármely két adategység közt csak egyetlenegy szeparátor jelenhet meg. Kivételt képez ezen szabály alól, ha az adott mezőhöz

vagy információs egységhez tartozó adat nem áll rendelkezésre, hiányzik, vagy opcionális, és a tranzakció feldolgozása nem függ az adott adat meglététől. Ezekben az esetekben több, egymás melletti szeparátor karakternek kell megjelennie, ahelyett, hogy közéjük áladatokat tennének.

Nézzük egy három információs egységből álló mező meghatározását. Amennyiben a második információs egységhez tartozó adat hiányzik, akkor a két egymás melletti „US”-információszeparátor karakter jelenik meg az első és a harmadik információs egység közt. Ha mind a második, mind a harmadik információs egység hiányzik, akkor három szeparátor karaktert kell használni – két „US”-karaktert a végződő mező- vagy almező-szeparátor karakteren kívül. Általánosságban, ha egy vagy több kötelező információs egység nem áll rendelkezésre az adott mezőnél vagy almezőnél, akkor a megfelelő számú szeparátor karaktert kell beilleszteni.

Elképzelhető a négy rendelkezésre álló szeparátor karakter közül kettő vagy több egymás melletti kombinációjának megjelenése. Ha egyes információs egységek, almezők vagy mezők esetén hiányoznak, vagy nem állnak rendelkezésre az adatok, a szükséges adategységek, almezők, vagy mezők számánál eggyel kevesebb szeparátor karakternek kell megjelennie.

1. Táblázat: Használt szeparátorok

Kód	Típus	Leírás	Hexadecimális érték	Decimális érték
US	Egységszeparátor	Információs egységeket választ el	1F	31
RS	Rekordszeparátor	Almezőket választ el	1E	30
GS	Csoportszeparátor	Mezőket választ el	1D	29
FS	Fájlszeparátor	Logikai rekordokat választ el	1C	28

2.2 A rekordok felépítése

A mezőcímkézett logikai rekordoknál minden használt információs mezőt ennek a szabványnak megfelelően kell megszámozni. Minden mező formátuma a logikai rekord típusának számából és az ezt követő pontból („.”), egy mezőszámból és az ezt követő kettőspontból („:”), majd a mezőhöz tartozó megfelelő információból áll. A mezőcímkézett szám bármilyen 1-9 számjegyű szám lehet a pont és a kettőspont közt. Egész számú mezőszámként értelmezendő. Ebből adódóan a „2.123:” mezőszám egyenértékű a „2.000000123:” mezőszámmal, és ugyanúgy értelmezendő.

Ebben a dokumentumban példaképp egy háromszámjegyű számot fogunk használni az itt leírt mezőcímkézett logikai rekordokban lévő fájlok megszámozásához. A mezőszámok formátuma „TT.yyy:” lesz, ahol „TT” az egy vagy két karakterből álló rekordtípust jelöli, és utána egy pont áll. A következő három karakter a megfelelő mezőszámot jelzi, utána egy kettőspont van. A kettőspont után jön a leíró ASCII-információ, vagy a képadatok.

Az 1. és 2. típusú logikai rekordok csak ASCII-szövegből álló adatmezőkből állnak. A rekord teljes hossza (beleértve a mezőszámokat, kettőspontokat és a szeparátor karaktereket) az egyes

rekordtípusokon belül az első ASCII-mezőként rögzítendő. Az „FS” ASCII fájlszeparátor karakter (amely a logikai rekord vagy a tranzakció végét jelöli) az ASCII információ utolsó karaktere után kell, hogy következzen, és bele kell számítani a rekord hosszába.

A mezőcímkézési koncepcióval ellentétben a 4. típusú rekordok csak bináris adatokat tartalmaznak, amelyeket sorba állított, fix hosszúságú bináris mezőkként rögzítenek. A rekord teljes hossza minden rekord első 4 bájtos bináris mezőjében rögzítendő. Ehhez a bináris rekordhoz sem a rekordszámot, illetve a pontot, sem a mezőazonosító számot és a kettőspontot nem kell rögzíteni. Továbbá, mivel ennek a rekordnak minden mezőhossza fix, vagy meghatározott, a négy szeparátor karakter („US”, „RS”, „GS”, vagy „FS”) egyike sem értelmezendő másként, mint bináris adat. A bináris rekordnál az „FS” karaktert nem kell rekordszeparátor vagy tranzakció végét jelentő karakterként használni.

3. 1. típusú logikai rekord: a fájl-fejléc

Ez a rekord a fájlstruktúrát, a fájltípust és más fontos információkat ír le. Az 1. típusú mezőkhöz használt karakterkészlet csak az információcseréhez használt 8-bites ANSI-kódot tartalmazza.

3.1 Az 1. típusú logikai rekord mezői

3.1.1 1.001 mező: a logikai rekord hossza (LEN)

Ez a mező tartalmazza az egész 1. típusú logikai rekord bájtjainak számát. A mező „1.001:”-gyel kezdődik, ezt követi a rekord teljes hossza, beleértve minden mező minden karakterét és az információszeparátorokat.

3.1.2 1.002 mező: Verziószám (VER)

Annak biztosítására, hogy a felhasználók tudják, melyik ANSI/NIST szabvány van használatban, ez a négybájtos mező jelöli a fájlt létrehozó szoftver vagy rendszer által alkalmazott szabvány verziószámát. Az első két bájt a főverzió referenciaszámát, a második kettő az alsóbbrendű módosítás számát mutatja. Az eredeti 1986-os szabvány például az első verziónak tekintendő, és „0010”-zel jelölik, míg a jelenlegi ANSI/NIST-ITL 1-2000 szabvány lesz a „0300”.

3.1.3 1.003 mező: fájltartalom (CNT)

Ez a mező felsorolja a fájl összes rekordját, és azt a sorrendet, amelyben a rekordok a logikai fájlon belül találhatóak. Egy vagy több almezőből áll, amelyek mindegyike két, az adott fájlban található egyetlen logikai rekordot leíró információs egységből áll. Az almezőket ugyanabban a sorrendben kell bevinni, mint ahogy a rekordokat rögzítik és átadják.

Az első almező első információs egysége „1”, ami az 1. típusú rekordra utal. Ezt követi a második információs egység, amely a fájl többi rekordjának számát jelöli. Ez a szám megegyezik az 1.003 mező fennmaradó almezőinek számával is.

A fennmaradó almezők mindegyikéhez egy rekordot társítanak a fájlon belül, és az almezők sorozata megfelel a rekorodok sorozatának. Mindegyik almező két információs egységet tartalmaz. Az első jelöli a rekord típusát. A második a rekord IDC-jét. Az „US” karakter a két információs egység elválasztására szolgál.

3.1.4 1.004 mező: a tranzakció típusa (TOT)

Ez a mező egy hárombetűs emlékeztetőt tartalmaz, amely a tranzakció típusát jelöli. Ezek a kódok eltérhetnek az ANSI/NIST szabvány más alkalmazásai által használtaktól.

CPS: bűnügyi lenyomatkeresés (*Criminal Print-to-Print Search*). Ez a tranzakció egy bűncselekményhez kapcsolódó rekordnak a lenyomat-adatbázisban való keresése. A személyek lenyomatait a fájlnak WSQ-tömörített képekként kell tartalmaznia.

Amennyiben **Nincs találat**, az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord

Amennyiben **Találat** van**,** az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord
⇒ 1-14 4. típusú rekord

A CPS TOT-ot az **A.6.1. Táblázat** foglalja össze (6. Függelék).

PMS: lenyomat és látens közti keresés (Print-to-Latent Search). Ezt a tranzakciót akkor használják, ha egy lenyomatkészletet az azonosítatlan látens képek adatbázisában kell keresni. A válasz a megcélzott AUAR-keresés **Találat/Nincs találat**-döntését tartalmazza. Ha több azonosítatlan látens van, több SRE-tranzakció lesz a válasz, tranzakcióként egy látenssel. A személyek lenyomatait a fájlnak WSQ-tömörített képekként kell tartalmaznia.

Amennyiben **Nincs találat**, az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord

Amennyiben **Találat** van**,** az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord
⇒ 1 13. típusú rekord

A PMS TOT-ot az **A.6.1. Táblázat** foglalja össze (6. Függelék).

MPS: látens és lenyomat közti keresés (*Latent-to-Print Search*). Ezt a tranzakciót akkor használják, ha egy látens képet a lenyomatok adatbázisában kell keresni. A fájlnak a látens sablont (*minutiae*) és a WSQ-tömörített képet kell tartalmaznia.

Amennyiben **Nincs találat**, az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord

Amennyiben **Találat** van**,** az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord
⇒ 1 4. típusú vagy 15. típusú rekord

Az MPS TOT-ot az **A.6.1. Táblázat** foglalja össze (6. Függelék).

MMS: látens és látens közti keresés (*Latent-to-Latent Search*). Ebben a tranzakcióban a fájl tartalmaz egy látenst, amelyet az azonosítatlan látens képek adatbázisában kell keresni, a különböző bűnügyi helyszínek közti kapcsolódások megállapítása érdekében. A fájlnak a látens sablon (*minutiae*)-információkat és a WSQ-tömörített képet kell tartalmaznia.

Amennyiben **Nincs találat**, az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord

Amennyiben **Találat** van**,** az alábbi logikai rekordokat kell válaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord
⇒ 1 13. típusú rekord

Az MMS TOT-ot az **A.6.4. Táblázat** foglalja össze (6. Függelék).

SRE: Ezt a tranzakciót a megcélzott szervezet ujjnyomat iránti kérelmekre adja válaszként. A válasz a megcélzott AUAR-keresés **Találat/Nincs találat**-döntését tartalmazza. Ha több jelölt van, több SRE-tranzakció lesz a válasz, tranzakciónként egy jelölttel.
Az SRE TOT-ot az **A.6.2. Táblázat** foglalja össze (6. Függelék).

ERR: Ezt a tranzakciót a megcélzott AUAR tranzakciós hiba jelöléseként adja válaszként. Tartalmaz egy üzenetmezőt (ERM), amely a feltárt hibát jelöli. Az alábbi logikai rekordokat kell váaszolni:

⇒ 1 1. típusú rekord
⇒ 1 2. típusú rekord

Az ERRT-ot az **A.6.3 Táblázat** foglalja össze (6. Függelék).

2. Táblázat: Tranzakciók lehetséges kódjai

Tranzakció típusa	Logikai rekord típusa					
	1	2	4	9	13	15
CPS	M	M	M	-	-	-
SRE	M	M	C	- (C látens találatok esetén)	C	C
MPS	M	M	-	M (1*)	M	-
MMS	M	M	-	M (1*)	M	-
PMS	M	M	M*	-	-	M*
ERR	M	M	-	-	-	-

Jelmagyarázat:
M = kötelező
M* = a két rekordtípus közül csak egyet tartalmazhat
O = opcionális
C = Feltéve, hogy van rendelkezésre álló adat
- = nem lehetséges
1* = feltételes másodlagos rendszerekre

3.1.5 1.005 mező: a tranzakció dátuma (DAT)

Ez a mező jelöli azt a dátumot, amikor a tranzakciót megkezdték, és meg kell felelnie az ISO-szabványok YYYYMMDD formátumú jelölésének, ahol YYYY az évet, MM a hónapot, DD pedig a hónap napját jelöli. Az egyszámjegyű számok elé 0-t kell tenni. Az „19931004” például 1993. október 4-ét jelöli.

3.1.6 1.006 mező: prioritás (PRY)

Ez az opcionális mező 1-től 9-ig terjedő skálán jelöli a kérelem prioritását. „1” a legmagasabb, „9” pedig a legalacsonyabb prioritás. A Végrehajtási megállapodásnak megfelelően az „1”-es tranzakciókat azonnal fel kell dolgozni.

3.1.7 1.007 mező: a megcélzott szervezet azonosítója (DAI)

Ez a mező a tranzakció által megcélzott szervezetet jelöli.
Két információs egységből áll, a következő formátumban: CC/*agency*.
Az első információs egység az ISO 3166-ban meghatározott, két alfanumerikus karakterből álló országkódot tartalmazza. A második egység, az *agency*, a szervezet legfeljebb 32 alfanumerikus karakterből álló, szabad szövegű megnevezését tartalmazza.

3.1.8 1.008 mező: a forrásszervezet azonosítója (ORI)

Ez a mező jelöli a fájl forrását, formátuma megegyezik a DAI-éval (1.007 mező).

3.1.9 1.009 mező: tranzakciós ellenőrzési szám (TCN)

Ez egy referenciacélokat szolgáló ellenőrzési szám. A számítógépnek kell generálnia, az alábbi formátumban: YYSSSSSSSSA
ahol YY a tranzakció éve, SSSSSSSS egy nyolcjegyű sorozatszám, A pedig a 2. függelékben leírt eljárással generált ellenőrző karakter. Ahol nem áll rendelkezésre TCN, az YYSSSSSSSS mezőt 0-kal kell feltölteni, az ellenőrző karakter képzése a fentivel megegyező módon történik.

3.1.10 1.010 mező: tranzakció-ellenőrzés válasz (TCR)

Ahol kiküldtek egy kérelmet, amire ez a válasz, ennek az opcionális mezőnek legalább a kérő üzenet tranzakciós ellenőrzési számát kell tartalmaznia, így formátuma megegyezik a TCN-évl (1.009 mező).

3.1.11 1.011 mező: szkennelési alapfelbontás (NSR)

Ez a mező jelzi a rendszer szkennelési alapfelbontását, amelyet a tranzakció kezdeményezője támogat. A felbontást két számjegy, majd egy tizedespont, végül megint két számjegy jelzi. A Szerződéshez kapcsolódó minden tranzakció esetén a rátának 500 pixel/inch-nek vagy 19,68 pixel/mm-nek kell lennie.

3.1.12 1.012 mező: névleges átadási felbontás (NTR)

Ez az ötbájtos mező jelzi az átadott képek névleges átadási felbontását. A felbontást az NSR-évl (1.011 mező) megegyező formátumban, pixel/mm-ben fejezik ki.

3.1.13 1.013 mező: doménnév (DOM)

Ez a kötelező mező jelöli a felhasználó által meghatározott 2. típusú logikai rekordokhoz használt doménnevet. Két információs egységből, áll, és „INT-I{US}4.22{GS}” kell, hogy legyen.

3.1.14 1.014 mező: greenwich-i középidő (GMT)

Ez a kötelező mező arra szolgál, hogy a greenwich-i középidő (GMT) egységeiben lehessen a dátumot és az időpontot kifejezni. Ha alkalmazzék, a GMT mező azt az univerzális dátumot tartalmazza, amely az 1.005 (DAT) mezőben lévő helyi dátumot egészíti ki. A GMT mező használata révén elkerülhetőek azok a helyiidő-inkonzisztenciák, amelyek abban az esetben lépnek fel, ha a tranzakció és az erre adott választ két, különböző időzónába tartozó hely között mozog. A GMT az időzónáktól független univerzális dátumot és 24 órás időmeghatározást biztosít. Formátuma „CCYYMMDDHHMMSSZ”, egy 15 karakterből álló sorozat, amely egy összefűzött GMT-dátum, a végén egy „Z”-vel. A „CCYY” karakterek jelölik a tranzakció évét, az „MM” karakterek a percet, az „SS” pedig a másodpercet. A teljes dátum nem lehet későbbi a jelenleginél.

4. 2. típusú logikai rekord: leíró szöveg

Ezen rekord nagy részének struktúráját nem az eredeti ANSI/NIST szabvány határozza meg. A rekord a fájlt küldő vagy fogadó szervezet érdeklődésére számot tartó információkat tartalmaz. Az egymással kommunikáló ujjnyomat-rendszerek kompatibilitásának biztosítására ez az ICD azt követeli meg, hogy a rekord csak az alábbiakban felsorolt mezőket tartalmazza. Ez a dokumentum írja le, hogy melyik mezők kötelezőek, és melyek opcionálisak, továbbá az egyedi mezők struktúráját is definiálja.

4.1 A 2. típusú logikai rekord mezői

4.1.1 2.001 mező: a logikai rekord hossza (LEN)

Ez a mező tartalmazza ennek a 2. típusú logikai rekord bájtjainak számát, és meghatározza a bájtok teljes számát, beleértve a rekordban lévő minden mező összes karakterét és az információ-szeparátorokat.

4.1.2 2.002 mező: képjelölési karakter (IDC)

Az ebben a kötelező mezőben lévő IDC az IDC egy ASCII-megjelenítése, az 1. típusú rekord fájltartalmi mezőjében meghatározottak szerint.

4.1.3 2.003 mező: rendszerinformáció (SYS)

Ez a mező kötelező, és négy bájtot tartalmaz, amelyek azt jelölik, hogy az adott 2. típusú rekord az INT-I mely verziójának felel meg. Az első két bájt jelöli a főverziószámot, a második kettő pedig az alsóbbrendű módosítás számát mutatja. Ez az alkalmazás például az INT-1 4. b verziójának 22. módosításán alapul, és „0422”-ként jelölik.

4.1.4 2.007 mező: esetszám (CNO)

Ezt a számot a helyi ujjnyomat-feldolgozó szervezet társítja a bűncselekmény helyszínén talált látensekkel. Formátuma a következő: CC/*szám*
ahol CC az Interpol országkódja, hossza két alfanumerikus karakter, a *szám* pedig a vonatkozó helyi irányelvekkel összhangban áll, és maximum 32 alfanumerikus karakterből áll. Ez a mező teszi lehetővé a rendszer számára, hogy beazonosítsa az adott bűncselekménnyel kapcsolatban álló látenseket.

4.1.5 2.008 mező: sorozatszám (SQN)

Ez jelöl egy ügyön belül minden látenssorozatot. Sorozat alatt olyan látenst, vagy látensek halmazát értjük, amelyeket a tárolás és/vagy a keresés szempontjából egybe csoportosítottak. Ebből a meghatározásból következik, hogy az egyedi látensekhez is kell sorozatszámot rendelni. Ezt a mezőt, az MID-vel (2.009 mező) együtt ki lehet tölteni, egy sorozaton belül egy adott látens azonosítására.

4.1.6 2.009 mező: látensazonosító (MID)

Ez jelöli egy sorozaton belül az egyedi látenst. Értéke egy betű, ahol ’A’-t rendelik az első, ’B’-t a második látenshez, és így tovább, egészen ’J’-ig. Ezt a mezőt az SQN (2.008 mező) leírásánál ismertetett látens-sorozatszámhoz hasonlóan kell használni.

4.1.7 2.010 mező: bűnügyi referenciaszám (CRN)

Ezt az egyedi referenciaszámot egy nemzeti hatóság rendeli hozzá egy olyan személyhez, akit először gyanúsítanak meg bűncselekmény elkövetésével. Egy országon belül egyetlen személynek sem lehet egynél több CRN-je, és két személynek sem lehet ugyanaz. Ugyanannak a személynek különböző országokban azonban lehetnek különböző bűnügyi referenciaszámai, amelyeket az országkód különböztet meg egymástól.

A CRN mező formátuma a következő: CC/*szám*
ahol CC az ISO 3166 szabvány szerinti országkód, hossza két alfanumerikus karakter, a *szám* pedig a vonatkozó helyi irányelvekkel összhangban áll, és maximum 32 alfanumerikus karakterből áll.

A Szerződéssel kapcsolatos tranzakciók esetén ezt a mezőt a származási szervezet nemzeti bűnügyi referenciaszámaként használják, amely a 4. vagy 15. típusú rekordokban lévő képekhez kapcsolódik.

4.1.8 2.012 mező: vegyes azonosítószám (MN1)

Ez a mező tartalmazza a CPS vagy PMS tranzakcióban átadott CRN-t (2.010 mező) az elején lévő országkód nélkül.

4.1.9 2.013 mező: vegyes azonosítószám (MN2)

Ez a mező tartalmazza az MPS vagy MMS tranzakcióban átadott CNO-t (2.007 mező) az elején lévő országkód nélkül.

4.1.10 2.014 mező: vegyes azonosítószám (MN3)

Ez a mező tartalmazza az MPS vagy MMS tranzakcióban átadott SQN-t (2.008 mező).

4.1.11 2.015 mező: vegyes azonosítószám (MN4)

Ez a mező tartalmazza az MPS vagy MMS tranzakcióban átadott MID-t (2.009 mező).

4.1.12 2.063 mező: további információk (INF)

Ez a legfeljebb 32 alfanumerikus karakterből álló opcionális mező további információkat tartalmazhat a kérelemről.

4.1.13 2.064 mező: válaszlista (RLS)

Ez a mező legalább két almezőt tartalmaz. Az első almező írja le egy hárombetűs, a TOT (1.004 mező) tranzakciós típusát jelölő emlékeztető használatával végrehajtott keresés típusát. A második almező egyetlen karakterből áll. „**I**” jelöli a TALÁLAT-ot, „**N**” pedig azt, hogy nem találtak egyező esetet (NINCS TALÁLAT). A harmadik almező az eredményként kapott jelölt sorozat-azonosítóját és – / jellel elválasztva – a jelöltek teljes számát. Ha több jelölt van, több üzenet lesz a válasz.

Lehetséges TALÁLAT esetén a negyedik almező tartalmazhatja – legfeljebb hat számjegyig – a pontszámot. Ha a TALÁLAT-ot visszaigazolják, az almező értéke „999999”.

Példa: "CPS{RS}I{RS}001/001{RS}999999{GS}"

Ha a távoli AUAR nem ad ki pontszámot, akkor a megfelelő ponton 0-s pontszámot kell alkalmazni.

4.1.14 2.074 mező: státusz-/hibaüzenet-mező (ERM)

Ez a mező tartalmazza a tranzakciókból eredő hibaüzeneteket, amelyeket a kérelmezőnek egy hibatranzakcióban küldenek vissza.

Számkód (1-3)	Jelentés (5-128)
003	HIBA: NEM ENGEDÉLYEZETT HOZZÁFÉRÉS
101	EGY KÖTELEZŐ MEZŐ HIÁNYZIK
102	ÉRVÉNYTELEN REKORDTÍPUS
103	MEGHATÁROZATLAN MEZŐ
104	MEGHALADJA AZ ELŐFORDULÁSOK MAXIMÁLIS SZÁMÁT
105	ÉRVÉNYTELEN SZÁMÚ ALMEZŐ
106	TÚL RÖVID MEZŐHOSSZ
107	TÚL HOSSZÚ MEZŐHOSSZ
108	A MEZŐ NEM AZ ELVÁRT SZÁM
109	A MEZŐSZÁM ÉRTÉKE TÚL ALACSONY
110	A MEZŐSZÁM ÉRTÉKE TÚL MAGAS
111	ÉRVÉNYTELEN KARAKTER
112	ÉRVÉNYTELEN DÁTUM
115	ÉRVÉNYTELEN EGYSÉGÉRTÉK
116	ÉRVÉNYTELEN TRANZAKCIÓTÍPUS
117	ÉRVÉNYTELEN REKORDADAT
201	HIBA: ÉRVÉNYTELEN TCN
501	HIBA: ELÉGTELEN UJJNYOMAT-MINŐSÉG
502	HIBA: HIÁNYZÓ UJJNYOMATOK
503	HIBA: AZ UJJNYOMAT-SOROZAT ELLENŐRZÉSE SIKERTELEN
999	HIBA: BÁRMILYEN MÁS HIBA. RÉSZLETEKÉRT HÍVJA A MEGCÉLZOTT SZERVEZETET!

Hibaüzenetek a 100 és 199 közti tartományban:

Ezek a hibaüzenetek az ANSI/NIST rekordok érvényesítésével kapcsolatosak, és az alábbiak szerint definiálódnak:
<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 egydileg egy konkrét hibaokhoz kapcsolódó kód (lásd táblázat)
- field_id a helytelen mező ANSI/NIST mezőszáma (pl. 1.001, 2.001, ...)
  a <record_type>.<field_id>.<sub_field_id> formátumban
- dynamic text a hiba egy részletesebb, dinamikus leírása
- LF egy sorelválasztó, amely több hiba esetén a hibákat elválasztja egymástól
- 1. típusú rekordokra az ICD-t "-1"-nek kell venni.

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

Ez a mező kötelező a hibatranzakciók esetében.

4.1.15 2.320 mező: jelöltek elvárt száma (ENC)

Ez a mező tartalmazza a kérelmező szervezet által az ellenőrzésre szánt jelöltek elvárt maximális számát. Az ENC értéke nem haladhatja meg a jelen Végrehajtási megállapodás B.2 Mellékletében meghatározott értékeket.

5. 4. típusú logikai rekord: nagyfelbontású szürkeskálás kép

Meg kell jegyezni, hogy a 4. típusú rekordok binárisak, és nem ASCII-jellegűek. Ezért a rekordon belül minden mezőhöz egy konkrét pozíció tartozik, azaz minden mező kötelező. A szabvány lehetővé teszi, hogy mind a képméretet, mind a felbontást meghatározzák a rekordon belül. A 4. típusú logikai rekordoknak a szabvány szerint olyan ujjnyomat-adatokat kell tartalmazniuk, amelyeket 500 és 520 pixel/inch közti névleges pixelsűrűséggel adnak át. Az új képek preferált felbontása 500 pixel/inch, vagy 19,68 pixel/mm. Az 500 pixel/inch-es sűrűséget az INT-I határozza meg, azzal az eltéréssel, hogy a hasonló rendszerek egymással egy nem preferált rátával is kommunikálhatnak, az 500 és 520 pixel/inch-es értékek között.

5.1 4. típusú logikai rekordok mezői

5.1.1 4.001 mező: a logikai rekord hossza (LEN)

Ez a négybájtos mező tartalmazza ennek a 4. típusú rekordnak a hosszát, és meghatározza a bájtok teljes számát, beleértve a rekordban lévő minden mező összes karakterét.

5.1.2 4.002 mező: képkijelölési karakter (IDC)

Ez a fejléc-fájlban megadott IDC-szám egybájtos bináris jelölése.

5.1.3 4.003 mező: nyomattípus (IMP)

A nyomattípus egy egyetlen bájtból álló mező, amely a rekord hatodik bájtján van.

3. táblázat : ujjnyomat-típusok

Kód	Leírás
0	Sima ujjnyomat élő képe
1	Körbe forgatott ujjnyomat élő képe
2	Sima ujjnyomat papírról átvett nem élő képe
3	Körbe forgatott ujjnyomat papírról átvett nem élő képe
4	Közvetlenül felvett látens-nyomat
5	Látens-nyomok
6	Látens fénykép
7	Latent lift
8	Swipe
9	Ismeretlen

5.1.4 4.004 mező: ujjpozíció (FGP)

Ez a fix hosszúságú 6 bájtos mező egy 4. típusú rekord 7-12. pozícióit fogalja el. A baloldali bájttól (a rekord 7. bájtja) kezdődően a lehetséges ujjpozíciókat tartalmazza. Az alábbi táblázat foglalja össze az ismert, vagy legvalószínűbb ujjpozíciót. Legfeljebb öt további ujjra lehet utalni, a fennmaradó öt bájtra további ujjpozíciók betöltésével, ugyanebben a formátumban. Ha ötnél kevesebb ujjpozíció-referenciára van szükség, a nem használt bájtokat a bináris 255-tel kell feltölteni. Minden ujjpozíció-referenciánál az ismeretlenre a 0-s kód használandó.

4. táblázat: Ujjpozíció-kódok és maximális méret

Ujjpozíció	Ujjkód	Szélesség (mm)	Hossz (mm)
Ismeretlen	0	40.0	40.0
Jobb hüvelykujj	1	45.0	40.0
Jobb mutatóujj	2	40.0	40.0
Jobb középső ujj	3	40.0	40.0
Jobb gyűrűsujj	4	40.0	40.0
Jobb kisujj	5	33.0	40.0
Bal hüvelykujj	6	45.0	40.0
Bal mutatóujj	7	40.0	40.0
Bal középső ujj	8	40.0	40.0
Bal gyűrűsujj	9	40.0	40.0

Ujjpozíció	Ujjkód	Szélesség (mm)	Hossz (mm)
Bal kisujj	10	33.0	40.0
Sima jobb hüvelyk	11	30.0	55.0
Sima bal hüvelyk	12	30.0	55.0
Sima jobb négy ujj	13	70.0	65.0
Sima bal négy ujj	14	70.0	65.0

A bűnügyi helyszíneken rögzített látenseknél csak a 0 és 10 közti kódok használandóak.

5.1.5 4.005 mező: képszkennelés felbontása (ISR)

Ez az egybájtos mező egy 4. típusú mező 13. bájtját foglalja el. Ha „0-„-t tartalmaz, akkor a képet a preferált 19,68 pixel/mm (500 pixel/inch)-es rátával dolgozták fel. Ha „1”-et tartalmaz, akkor a képet az 1. típusú rekordban specifikált alternatív szkennelési rátával dolgozták fel.

5.1.6 4.006 mező: horizontális sorhosszúság (HLL)

Ez a mező a 4. típusú rekordon belül a 14. és 15. bájtokon található. A szkennelési sorokban lévő pixelek számát tartalmazza. Az első bájt a legfontosabb.

5.1.7 4.007 mező: függőleges sorhosszúság (VLL)

Ez a mező a 16. és 17. bájtban a képben jelen lévő szkennelési sorok számát tartalmazza. Az első bájt a legfontosabb

5.1.8 4.008 mező: szürkeskálás tömörítési algoritmus (GCA)

Ez az egybájtos mező a képadat kódolásához használt szürkeskálás tömörítési algoritmust jelöli. A bináris zéró azt jelzi, hogy nem használtak tömörítési algoritmust. Ebben az esetben a pixeleket balról jobbra, fentről lefelé rögzítik. Az FBI működteti a nem zéró számok tömörítési algoritmusoknak való megfeleltetését. Az INT-I alapú alkalmazás ugyanezeket a számmegfeleltetéseket alkalmazza.

5.1.9 4.009 mező: a kép

Ez a mező egy, a képet jelölő bájtsorozatot tartalmaz. Struktúrája természetesen az alkalmazott tömörítési algoritmustól függ.

6. 9. típusú logikai rekord: minutiae-rekord

A 9. típusú rekordok a minutiákat és az ehhez kapcsolódó, egy látensből kódolt információkat leíró ASCII-szöveget tartalmazzák. A látenskeresési tranzakciókra nincsen korlátozva az egy fájlban lévő ilyen 9. típusú rekordok száma. Mindegyiküknek más-más nézethez vagy látenshez kell tartoznia.

6.1 Minutia-kicsomagolás

6.1.1 Minutia-típusazonosítás

Ez a standard három azonosítót határoz meg, amelyeket a minutia típusának leírására használnak. Ezeket a 4.1 táblázat tartalmazza. A redővéget 1. típusúnak kell jelölni. A redők kettéválását 2. típusúnak kell jelölni. Ha egy sablont nem lehet egyértelműen a fenti két típus egyikébe besorolni, akkor „egyéb”-ként, 0. típusúnak kell jelölni.

5. táblázat: Sablontípusok

Típus	Leírás
0	Egyéb
1	Redővég
2	Redők kettéválása

6.1.2 Minutiaelhelyezés és -típus

Az ANSI INCITS 378-2004 szabványnak megfelelő minutiasablonok esetén a jelenlegi INCITS 378-2004 szabványt továbbfejlesztő alábbi eljárást kell alkalmazni az egyedi minutiák elhelyezésének (helyzetének és szögirányának) meghatározására.

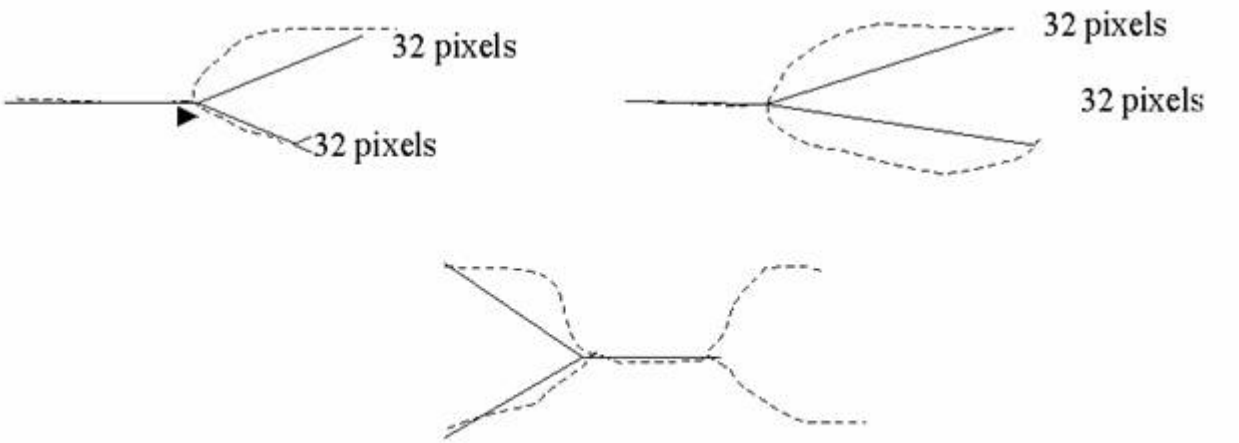
Egy redővéget jelölő minutia helyzete vagy elhelyezkedése a közvetlenül a redővég előtt lévő völgyterület középső bordázatának kettéválási pontja kell, hogy legyen. Ha a völgyterület három szárát egy-egy pixel szélességű bordázattá csökkentenénk, a metszéspont lenne a minutia elhelyezkedése. Hasonlóan, egy kettéválás minutiája a redő középső bordázatának kettéválási pontján helyezkedik el. Ha a völgyterület három szárát egy-egy pixel szélességű bordázattá csökkentenénk, a három szár metszéspontja lenne a minutia elhelyezkedése.

Miután minden redővéget kettéválásokká alakítottak át, az ujjnyomat-kép minden minutiáját kettéválásokként jelölik. Minden minutia három szára metszetének X és Y pixelkoordinátáját közvetlenül lehet megformázni. A minutia irányát minden bordázat-kettéválásból meg lehet határozni. Minden bordázat-kettéválás három szárát meg kell vizsgálni, és minden szár végpontját meg kell határozni. A 6.1.2 ábra a szár végződésének meghatározásához használt módszereket foglalja össze, egy 500 ppi-s szkennelési felbontást alapul véve.

A végződést az elsőként bekövetkező esemény alapján határozzák meg. A pixelek száma egy 500 ppi-s szkennelési felbontást vesz alapul. Eltérő szkennelési felbontások eltérő pixelszámot eredményeznek.

- 0,064 inch távolság (a 32. pixel)
- A 0,02 inch és 0,064 inch távolságok (10-32. pixelek) közt előforduló bordázatszár vége; a rövidebb szárakat nem használják
- 0,064 inch távolságon belül (a 32. pixel előtt) egy második kettéválás található

6.1.2 ábra



A minutiák szöge három, a kettéválási pontból induló és minden szár végéig húzódó virtuális sugár szerkesztésével határozható meg. A sugarak által befogott szögek legkisebbikének felezője jelöli a minutia irányát.

6.1.3 Koordinátarendszer

Az ujjnyomat minutiáinak kifejezéséhez a Descartes-féle koordinátarendszert kell használni. A minutiák elhelyezkedését x és y koordinátáik jelölik. A koordinátarendszer origója az eredeti kép bal felső sarka, ahonnan x jobbra, y pedig lefelé növekszik. A minutia x és y koordinátáit egyaránt az origótól számított pixelegységben kell kifejezni. Megjegyzendő, hogy az origó elhelyezkedése és a mértékegységek nem állnak összhangban az ANSI/NIST-ITL 1-2000-ben leírt 9. típus definícióival.

6.1.4 Minutiák iránya

A szögeket szokványos matematikai formában, jobbra 0 fokban, az óramutató járásával ellentétes szögnövekedéssel fejezik ki. Redővégnél a mért szögek a redő irányába visszafelé, kettéválásánál a völgy közepe felé irányulnak. Ez az ANSI/NIST-ITL 1-2000-ben leírt 9. típus definícióiban rögzített szögmegállapodáshoz képest 180 fokos eltérést jelent.

6.2 A 9. típusú logikai rekord INCITS-378 formátumának mezői

A 9. típusú rekordok minden mezőjét ASCII-szövegként kell rögzíteni. Ebben a mezőcímkézett rekordban nem megengedettek a bináris mezők.

6.2.1 9.001 mező: a logikai rekord hossza (LEN)

Ez a kötelező ASCII mező tartalmazza ezen logikai rekord hosszát, és meghatározza a bájtok teljes számát, beleértve a rekordban lévő minden mező összes karakterét.

6.2.2 9.002 mező: képkijelölési karakter (IDC)

Ez a kötelező kétbájtos mező a minutiák adatainak beazonosítására és elhelyezésére szolgál. Az ebben a mezőben lévő IDC meg kell, hogy egyezzen az 1. típusú rekord fájltartalom-mezőjében lévő IDC-vel.

6.2.3 9.003 mező: nyomattípus (IMP)

Ez a kötelező egybájtos mező írja le az ujjnyomatkép-információ beszerzésének módját. A 3.1 táblázatból kiválasztott megfelelő kód ASCII értékét kell ebbe a mezőbe bevinni, a nyomattípus megjelölésére.

6.2.4 9.004 mező: minutia-formátum (FMT)

Ez a mező egy ”U”-t tartalmaz, annak jelölésére, hogy a minutiákat az M1-378 szabvány szerint formázták. Bár az információkat lehet az M1-378 szabvány szerint kódolni, a 9. típusú rekord minden adatmezője ASCII szövegmező kell, hogy maradjon.

6.2.5 9.126 mező: CBEFF információ

Ez a mező három információs egységet tartalmaz. Az első információs egység a „27”(0x1B) értéket tartalmazza. Ez a Nemzetközi Biometrikai Ipari Társaság (*International Biometric Industry Association* – IBIA) által az INCITS M1 Technikai Bizottságába kijelölt CBEFF-formátumtulajdonos azonosítója. Az <US> karakter választja el ezt az egységet a CBEFF-formátumtípustól, ami az „513” (0x0201) értéket kapja, annak jelölésére, hogy ez a rekord csak az elhelyezkedésre és a szögirányra vonatkozó adatot tartalmaz, és semmilyen kiterjesztett adatblokkra (*Extended Data Block*) vonatkozót. Az <US> karakter választja el ezt az egységet a CBEFF-termékazonosítótól (PID), amely a kódoló berendezés „tulajdonosát’ azonosítja. Az eladó állapítja meg ennek értékét. Az IBIA honlapjáról (www.ibia.org) tudható meg, amennyiben ott szerepel.

6.2.6 9.127 mező: a képrögzítő berendezés azonosítója

Ez a mező két, egymástól az <US> karakterrel elválasztott információs egységet tartalmaz. Az elsőben „APPF” kell, hogy szerepeljen, ha a kép beszerzésére eredetileg használt berendezés tanúsítottan megfelel a CJIS-RS-0010, az amerikai Szövetségi Nyomozóiroda (FBI) elektronikus ujjnyomat-átadási specifikációja F Függelékének (IAFIS képminőség-specifikáció, 1999. január 29.). Ha a berendezés nem felelt meg ennek, a mező értéke „NONE” lesz. A második információs egységnek kell tartalmaznia a képrögzítő berendezés azonosítóját, amely a képrögzítő berendezés egy eladó által kijelölt termékszáma. A „0” érték azt jelöli, hogy a képrögzítő berendezés azonosítója ismeretlen.

6.2.7 9.128 mező: vízszintes sorhosszúság (HLL)

Ez a kötelező ASCII mező jelöli az átadott kép egyetlen vízszintes sorában lévő pixelek számát. A maximális vízszintes sorhosszúság 65534 pixel.

6.2.8 9.129 mező: függőleges sorhosszúság (VLL)

Ez a kötelező ASCII mező jelöli az átadott képben lévő vízszintes sorok számát. A maximális függőleges sorhosszúság 65534 pixel.

6.2.9 9.130 mező: skálaegységek (SLC)

Ez a kötelező ASCII mező jelöli a képfeldolgozási frekvencia (pixelsűrűség) leírására használt egységeket. A mezőben lévő „1”-es a pixel/inch, a „2”-es pedig a pixel/cm. A „0” azt jelöli, hogy nincs megadva skála. Ebben az esetben a HPS/VPS arány adja meg a pixelarányt.

6.2.10 9.131 mező: vízszintes pixelskála (HPS)

Ez a kötelező ASCII mező jelöli a vízszintes irányban használt egészszámú pixelsűrűséget, feltéve, hogy az SLC tartalma „1” vagy „2”. Ellenkező esetben a pixel-oldalarány vízszintes komponensét jelöli.

6.2.11 9.132 mező: függőleges pixelskála (VPS)

Ez a kötelező ASCII mező jelöli a függőleges irányban használt egészszámú pixelsűrűséget, feltéve, hogy az SLC tartalma „1” vagy „2”. Ellenkező esetben a pixel-oldalarány függőleges komponensét jelöli.

6.2.12 9.133 mező: ujjnézet

Ez a kötelező mező az ezen rekordban lévő adatokhoz társított ujj nézetszámát jelöli. A nézetszám „0”-val kezdődik, és egyesével nő „15”-ig.

6.2.13 9.134 mező: ujjpozíció (FGP)

Ez a mező tartalmazza az ebben a 9. típusú rekordban lévő információt megalapozó ujjpozíciót jelölő kódot. Az ujj vagy a tenyér pozícióját a 3.2 táblázatban leírt, 1 és 10 közötti kódok, illetve a 6.3 táblázat megfelelő tenyérkódjai jelölik.

6.2.14 9.135 mező: ujjminőség

Ez a mező tartalmazza az összes ujjminutia-adat minőségét, értéke 0 és 100 között lehet. A szám az ujjrekord minőségének átlagos kifejezése, az eredeti kép, a minutia-kivonat és bármely további, a minutiarekordra ható művelet minőségét jelöli.

6.2.15 9.136 mező: minutiák száma

Ez a kötelező mező az ebben a rekordban lévő minutiák számát jelöli.

6.2.16 9.137 mező: ujjminutiák adatai

Ebben a kötelező mezőben hat információs egység van, amelyeket az <US> karakter választ el egymástól. Több almezőből áll, amelyek mindegyike egyetlen minutia részleteit tartalmazza. A

minutia-almezők teljes száma meg kell, hogy egyezzen a 136-os mezőben található számmal. Az első információs egység a minutia indexszáma, amelyet „21”-gyel kell kezdeni, és „1”-gyel növelni az ujjnyomatban lévő minden további minutiánál. A második és a harmadik információs egység a minutia pixelegységekben kifejezett ’x’ és ’y’ koordinátája. A negyedik információs egység a minutiák kétfokos egységekben mért szöge. Ez a nemnegatív érték 0 és 179 közt lehet. Az ötödik információs egység a minutia típusa. A „0” érték az „EGYÉB” típusú minutiát, az „1” a redővéget, a „2” pedig a redő-kettáválást jelöli. A hatodik információs egység az egyes minutiák minőségét jelöli. Ez az érték 1-től (minimális) 100-ig (maximális) terjedhet. A „0” érték azt jelöli, hogy nem áll rendelkezésre minőségérték. Minden almezőt az <RS> szeparátorkarakter választ el a következőtől.

6.2.17 9.138 mező: redők számára vonatkozó információ

Ez a mező almezők sorozatából áll, amelyek mindegyike három információs egységet tartalmaz. Az első almező első információs egysége a redők számának megállapítására használt módszert jelöli. A „0” azt jelöli, hogy nem lehet megállapítani a redők számának megállapítására használt módszert, sem pedig sorrendjüket a rekordon belül. Az „1” azt jelöli, hogy minden központi minutiában a redők számát a legközelebbi szomszédos minutiába négy kvadránsban dolgozták fel, és minden központi minutia redőszáma egyben van felsorolva. A „2” azt jelöli, hogy minden központi minutiában a redők számát a legközelebbi szomszédos minutiába nyolc oktánsban dolgozták fel, és minden központi minutia redőszáma egyben van felsorolva. Az első almező fennmaradó két információs egysége egyaránt „0”-t tartalmaz. Az információs egységeket az <US> szeparátorkarakterrel kell elválasztani egymástól. A további almezők első információs egysége a központi minutia indexszámát, második információs egysége a szomszédos minutiák indexszámát, harmadik információs egysége pedig az egymást keresztező redők számát tartalmazza. Az almezőket az <RS> szeparátorkarakterrel kell elválasztani egymástól.

6.2.18 9.139 mező: maginformáció

Ez a mező minden, az eredeti képen jelen lévő maghoz rendelt egy-egy almezőből áll. Mindegyik almező három információs egységből áll. Az első két egység a pixelegységekben kifejezett ’x’ és ’y’ koordináta-pozíciókat tartalmazza. A harmadik információs egység a mag 2 fokos egységekben mért szögét tartalmazza. Ez a nemnegatív érték 0 és 179 közt lehet. Több mag esetén az <RS> szeparátorkarakter választja el őket.

6.2.19 9.140 mező: deltainformáció

Ez a mező minden, az eredeti képen jelen lévő deltához rendelt egy-egy almezőből áll. Mindegyik almező három információs egységből áll. Az első két egység a pixelegységekben kifejezett ’x’ és ’y’ koordináta-pozíciókat tartalmazza. A harmadik információs egység a delta 2 fokos egységekben mért szögét tartalmazza. Ez a nemnegatív érték 0 és 179 közt lehet. Több mag esetén az <RS> szeparátorkarakter választja el őket.

7. 13. típusú változó felbontású látenskép-rekord

A 13. típusú mezőcímkézett logikai rekord a látens képekből nyert képadatokat tartalmazza. Ezen képeket az olyan szervezeteknek való átadásra szánják, amelyek azokat automatikusan, vagy emberi közreműködéssel feldolgozzák, hogy a képekből a kívánt információkat kinyerjék. Az alkalmazott szkennelési felbontásra vonatkozó információkat és a kép feldolgozásához szükséges további paramétereket a rekordon belül címkézett mezőkben rögzítik.

7. táblázat: A 13. típusú változó felbontású látensrekord felépítése

Azonosító	Kondíciós kód	Mezőszám	Mezőnév	Karakter-típus	Mezőméret előfordulásonként		Előfordulások száma		Bájtok maximális száma
					min.	max.	min.	max.	
LEN	M	13.001	LOGIKAI REKORD HOSSZA	N	4	8	1	1	15
IDC	M	13.002	KÉPKIJELÖLÉSI KARAKTER	N	2	5	1	1	12
IMP	M	13.003	LENYOMATTÍPUS	A	2	2	1	1	9
SRC	M	13.004	FORRÁSSZERVEZET/ ORI	AN	6	35	1	1	42
LCD	M	13.005	LÁTENS FELVÉTELÉNEK DÁTUMA	N	9	9	1	1	16
HLL	M	13.006	VÍZSZINTES SORHOSSZÚSÁG	N	4	5	1	1	12
VLL	M	13.007	FÜGGŐLEGES SORHOSSZÚSÁG	N	4	5	1	1	12
SLC	M	13.008	SKÁLAEGYSÉGEK	N	2	2	1	1	9
HPS	M	13.009	VÍZSZINTES PIXELSKÁLA	N	2	5	1	1	12
VPS	M	13.010	FÜGGŐLEGES PIXELSKÁLA	N	2	5	1	1	12
CGA	M	13.011	TÖMÖRÍTÉSI ALGORITMUS	A	5	7	1	1	14
BPX	M	13.012	BIT/PIXEL	N	2	3	1	1	10
FGP	M	13.013	UJJPOZÍCIÓ	N	2	3	1	6	25
RSV		13.014 13.019	FENNTARTVA KÉSŐBBI DEFINIÁLÁSRA	--	--	--	--	--	--
COM	O	13.020	KOMMENTÁR	A	2	128	0	1	135
RSV		13.021 13.199	FENNTARTVA KÉSŐBBI DEFINIÁLÁSRA	--	--	--	--	--	--

Azonosító	Kondíciós kód	Mezőszám	Mezőnév	Karakter-típus	Mezőméret előfordulásonként		Előfordulások száma		Bájtok maximális száma
					min.	max.	min.	max.	
UDF	O	13.200 13.998	FELHASZNÁLÓ ÁLTAL DEFINIÁLT MEZŐK	--	--	--	--	--	--
DAT	M	13.999	KÉPADATOK	B	2	--	1	1	--

Jelmagyarázat a karaktertípushoz: N = szám; A = betű; AN = alfanumerikus; B = bináris

7.1 A 13. típusú logikai rekord mezői

Az alábbi bekezdések írják le a 13. típusú logikai rekord mezői összes mezőjének adatait.

Egy 13. típusú logikai rekordon belül az adatokat számozott mezőkben kell bevinni. A rekord első két mezőjét sorrendbe kell tenni, a képadatokat tartalmazó mező kell, hogy a rekord utolsó fizikai mezője legyen. A 13. típusú rekordok minden mezőjéhez az 5.1 táblázat sorolja fel a „kondíciós kódokat” („M”=kötelező, vagy „O”=opcionális), a mezőszámot, a mezőnevet, a karaktertípust, a mezőméretet és az előfordulási korlátokat. Egy háromszámjegyű mezőszámot alapul véve a mező maximális bájtszámát az utolsó oszlop adja meg. Ha a mezőszámra több számjegyet használnak, a maximális bájtszám is nőni fog. Az „előfordulásonkénti mezőméretben” lévő két adat a mezőben használt összes karakterszeparátort tartalmazza. A „maximális bájtszámba” beletartozik a mezőszám, az információ és az összes karakterszeparátor, beleértve a „GS” karaktert.

7.1.1 13.001 mező: a logikai rekord hossza (LEN)

Ez a kötelező ASCII mező jelöli a 13. típusú logikai rekordban lévő bájtok teljes számát. A 13.001 mező jelöli a rekord hosszát, beleértve a rekordban lévő minden mező minden karakterét és az információ-szeparátorokat.

7.1.2 13.002 mező: képkijelölési karakter (IDC)

Ez a kötelező ASCII mező a rekordban lévő látenskép-adatok azonosítására szolgál. Az IDC-nek meg kell egyeznie az 1. típusú rekord fájltartalom (CNT) mezőjében található IDC-vel.

7.1.3 13.003 mező: nyomattípus (IMP)

Ez a kötelező, egy- vagy kétbájtos ASCII mező jelöli a látensképre vonatkozó információ megszerzésnek módját. A 3.1 (ujj), illetve az 5.3 (tenyér) táblázatból kiválasztott megfelelő látenskódot kell ebbe a mezőbe bevinni.

7.1.4 13.004 mező: forrásszervezet / ORI (SRC)

Ez a kötelező ASCII mező jelöli annak a hatóságnak vagy szervezetnek az azonosítóját, amelyik eredetileg rögzítette a rekordban lévő arcképet. Alapesetben a képet rögzítő szervezet Származási

Szervezet Azonosítója (*Originating Agency Identifier* – ORI) lesz ebben a mezőben. Két információs egységből áll, az alábbi formátumban: CC/*szervezet.*

Az első információs egység a két alfanumerikus karakterből álló Interpol-országkódot tartalmazza. A második egység (szervezet) a szervezet legfeljebb 32 alfanumerikus karakterből álló szabad szöveges azonosítója.

7.1.5 13.005 mező: a látens felvételének dátuma (LCD)

Ez a kötelező ASCII mező jelöli azt a dátumot, amikor a rekordban lévő látensképet felvették. A dátum nyolc számjegyből áll, CCYYMMDD formátumban. A CCYY karakterek azt az évet jelölik, amikor a képet felvették, az MM karakterek a hónap tízes és egyes helyiértékeit, a DD karakterek pedig a hónap napjának tízes és egyes helyiértékeit. Így például 20000229 2000. február 29-ét jelöli. A teljes dátumnak egy érvényes dátumnak kell lennie.

7.1.6 13.006 mező: vízszintes sorhosszúság (HLL)

Ez a kötelező ASCII mező jelöli az átadott kép egyetlen vízszintes sorában lévő pixelek számát.

7.1.7 13.007 mező: függőleges sorhosszúság (VLL)

Ez a kötelező ASCII mező jelöli az átadott kép egyetlen függőleges sorában lévő pixelek számát.

7.1.8 13.008 mező: skálaegységek (SLC)

Ez a kötelező ASCII mező jelöli a képfeldolgozás frekvenciájának (a pixelsűrűségnek) leírásához használt mértékegységet. Az ebben a mezőben lévő „1”-es pixel/inch-et, a „2”-es pedig pixel/cm-t jelöl. A „0” ebben a mezőben azt jelöli, hogy nincs megadva skála. Ebben az esetben a HPS/VPS hányados adja meg a pixel-oldalarányt.

7.1.9 13.009 mező: vízszintes pixelskála (HPS)

Ez a kötelező ASCII mező jelöli a vízszintes irányban használt egészszámú pixelsűrűséget, feltéve, hogy az SLC tartalma „1” vagy „2”. Ellenkező esetben a pixel-oldalarány vízszintes komponensét jelöli.

7.1.10 13.010 mező: függőleges Pixelskála (VPS)

Ez a kötelező ASCII mező jelöli a függőleges irányban használt egészszámú pixelsűrűséget, feltéve, hogy az SLC tartalma „1” vagy „2”. Ellenkező esetben a pixel-oldalarány függőleges komponensét jelöli.

7.1.11 13.011 mező: tömörítési algoritmus (CGA)

Ez a kötelező ASCII mező jelöli a szürkeskálás képek tömörítésére használt algoritmust.

8. táblázat: tömörítési kódok

Tömörítés típusa	Kód
Nincs tömörítés	NONE
Wavelet/Scalar Quantization (IAFIS-IC-0110)	WSQ
JPEG 2000	J2K

7.1.12 13.012 mező: bit/pixel (BPX)

Ez a kötelező ASCII mező jelöli egy pixel ábrázolásához használt bitek számát. A normális, „0” és „255” közti szürkeskálás értékekre a mező „8”-at tartalmaz. Az ebben a mezőben lévő bármely, 8-nál nagyobb szám megnövelt precizitású szürkeskálás pixelt jelöl.

7.1.13 13.013 mező: ujj/tenyér-pozíció (FGP)

Ez a kötelező, címkézett mező a látensképpel egyező egy vagy több lehetséges ujj- vagy tenyérpozíciót tartalmazza. Az ismert, vagy legvalószínűbb ujjpozíciónak megfelelő decimális kódszámot a 3.2-es, a legvalószínűbb tenyérpozíciót pedig az 5.3 táblázatból kell venni, és egy- vagy kétkarakteres ASCII-almezőként bevinni. A további ujj- és/vagy tenyérpozíciókra az alternatív pozíciókódok almezőként, az „RS” szeparátor-karakterrel elválasztva történő bevitelével lehet hivatkozni. Az „ismeretlen ujjat” jelölő „0” kódot minden, 1-től 10-ig terjedő ujjpozícióra alkalmazni kell. Az „ismeretlen tenyeret” jelölő „20”-as kódot minden felsorolt tenyérnyomat-pozícióra alkalmazni kell.

7.1.14 13.014-019 mezők: fenntartva későbbi definiálásra (RSV)

Ezek a mezők ezen szabvány későbbi módosításaiba való beillesztésre vannak fenntartva. A jelenlegi verzióban egyik mezőt sem kell használni. Ha mégis bármelyikük jelen van, nem kell figyelembe venni.

7.1.15 13.020 mező: kommentár (COM)

Ezt az opcionális mezőt kommentár, vagy más ASCII szöveges információnak a látenskép-adatokhoz való beillesztésére lehet használni.

7.1.16 13.021-199 mezők: fenntartva későbbi definiálásra (RSV)

Ezek a mezők ezen szabvány későbbi módosításaiba való beillesztésre vannak fenntartva. A jelenlegi verzióban egyik mezőt sem kell használni. Ha mégis bármelyikük jelen van, nem kell figyelembe venni.

7.1.17 13.200-998 mezők: felhasználó által definiált mezők (UDF)

Ezek a mezők a felhasználó által definiálhatóak. Méretüket és tartalmukat a felhasználó határozza meg, és összhangban kell állniuk a fogadó szervezettel. Ha használják őket, ASCII szöveges információkat tartalmaznak.

7.1.18 13.999 mező: képadatok (DAT)

Ez a mező egy felvett látenskép összes adatát tartalmazza. Mindig a 999-es mezőszámot kell hozzárendelni, és a rekord utolsó fizikai mezőjének kell lennie. A „13.999:”-t például egy binárisan jelölt képadat követ

Alapesetben a tömörítetlen szürkeskálás adatok minden pixelét nyolc bitre (256 szürke színárnyalatra) kell méretezni. Ha a BPX mezőben levő érték nagyobb vagy kisebb, mint „8”, a pixel leírásához szükséges bájtok száma eltérő lesz. Tömörítés esetén a pixeladatokat a GCA mezőben meghatározott tömörítési eljárással kell tömöríteni.

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

A konzisztencia érdekében a 13.999 mező adatai után közvetlenül egy „FS” szeparátort kell használni a következő logikai rekordtól való elválasztására. A szeparátort bele kell érteni a 13. típusú rekord hosszúsági mezőjébe.

8. 15. típusú változó felbontású tenyérnyomat-kép rekord

A 15. típusú mezőcímkézett logikai rekordot a tenyérnyomatkép-adatoknak a digitalizált képhez tartozó fix illetve a felhasználó által meghatározott szöveges információs mezőkkel együtt történő tárolására és cseréjére kell használni. Az alkalmazott szkennelési felbontásra, a képméretre, és más, a kép feldolgozásához szükséges paraméterekre vagy kommentárokra vonatkozó információkat a rekordon belül címkézett mezőként kell rögzíteni. A más szervezeteknek átadott tenyérnyomat-képeket a fogadó szervezet dolgozza fel, hogy egyeztetés céljából kinyerje belőle a kívánt információkat.

A képadatokat közvetlenül az adatalanytól kell beszerezni, egy *live-scan* készülékkel, vagy egy tenyérnyomat-kártyáról, illetve egyéb, az adatalany tenyérnyomatait tartalmazó adathordozóról.

Bármely, a tenyérnyomat-képek beszerzésre használt módszernek képesnek kell lennie mindkét kézről egy képsorozat rögzítésére. Ennek a készletnek tartalmaznia kell a tenyérnek az írás során az asztalhoz érő részét egyetlen szkennelt képben, és az egész tenyér teljes területét a csuklótól az ujjbegyekig egy vagy két szkennelt képben. Ha két képet használnak a teljes tenyér ábrázolására, az alsó képnek a csuklótól az ujjak közti területig (a harmadik ujjtőig) kell terjednie, és tartalmaznia kell az ujjpárnákat és a tenyér ez alatti területeit. A felső képnek az ujjak közötti területtől az ujjak első begyeiig kell terjednie. A közös terület redőszerkezetének és részleteinek egyeztetése révén a szemlélőnek egyértelműen ki kell tudnia jelenteni, hogy a két kép ugyanazt a tenyeret ábrázolja.

Mivel az ujjnyomat-tranzakciót különböző célokra lehet használni, a tenyérből vagy a kézből felvett egy vagy több egyedi képterületet tartalmazhat. Egy személy teljes tenyérnyomat-rekord-készlete általában a tenyérnek az írás során az asztalhoz érő részét és minden kézről a teljes tenyérképe(ke)t tartalmazza. Mivel egy mezőcímkézett logikai képrekord csak egy bináris mezőt tartalmazhat, egyetlen 15. típusú rekord szükséges minden, a tenyérnek az írás során az asztalhoz érő részéhez, és egy vagy két 15. típusú rekord minden teljes tenyérhez. Ezért 4-6 darab 15. típusú rekord szükséges az adatalany tenyérnyomatának rögzítéséhez egy normális tenyérnyomat-tranzakció során.

8.1 A 15. típusú logikai rekord mezői

Az alábbi bekezdések a 15. típusú logikai rekord mezőiben lévő adatokat írják le.

Egy 13. típusú logikai rekordon belül az adatokat számozott mezőkben kell bevinni. A rekord első két mezőjét sorrendbe kell tenni, a képadatokat tartalmazó mező kell, hogy a rekord utolsó fizikai mezője legyen. A 13. típusú rekordok minden mezőjéhez az 5.1 táblázat sorolja fel a „kondíciós kódokat” („M”=kötelező, vagy „O”=opcionális), a mezőszámot, a mezőnevet, a karaktertípust, a mezőméretet és az előfordulási korlátokat. Egy három számjegyű mezőszámot alapul véve a mező maximális bájtszámát az utolsó oszlop adja meg. Ha a mezőszámra több számjegyet használnak, a maximális bájtszám is nőni fog. Az „előfordulásonkénti mezőméretben” lévő két adat a mezőben használt összes karakterszeparátort tartalmazza. A „maximális bájtszámba” beletartozik a mezőszám, az információ és az összes karakterszeparátor, beleértve a „GS” karaktert.

8.1.1 15.001 mező: a logikai rekord hossza (LEN)

Ez a kötelező ASCII mező jelöli a 15. típusú logikai rekordban lévő bájtok teljes számát. A 15.001 mező jelöli a rekord hosszát, beleértve a rekordban lévő minden mező minden karakterét és az információ-szeparátorokat.

8.1.2 15.002 mező: képkijelölési karakter (IDC)

Ez a kötelező ASCII mező a rekordban lévő tenyérnyomat-kép azonosítására szolgál. Az IDC-nek meg kell egyeznie az 1. típusú rekord fájltartalom (CNT) mezőjében található IDC-vel.

8.1.3 15.003 mező: nyomattípus (IMP)

Ez a kötelező, egybájtos ASCII mező jelöli a tenyérnyomat-képre vonatkozó információ megszerzésnek módját. A 6.2 táblázatból kiválasztott megfelelő kódot kell ebbe a mezőbe bevinni.

8.1.4 15.004 mező: forrásszervezet / ORI (SRC)

Ez a kötelező ASCII mező jelöli annak a hatóságnak vagy szervezetnek az azonosítóját, amelyik eredetileg rögzítette a rekordban lévő arcképet. Alapesetben a képet rögzítő szervezet Származási Szervezet Azonosítója (*Originating Agency Identifier* – ORI) lesz ebben a mezőben. Két információs egységből áll, az alábbi formátumban: CC/*szervezet.*

Az első információs egység a két alfanumerikus karakterből álló Interpol-országkódot tartalmazza. A második egység (*szervezet*) a szervezet legfeljebb 32 alfanumerikus karakterből álló szabad szöveges azonosítója.

8.1.5 15.005 mező: a tenyérnyomat felvételének dátuma (PCD)

Ez a kötelező ASCII mező jelöli azt a dátumot, amikor a rekordban lévő tenyérnyomatot felvették. A dátum nyolc számjegyből áll, CCYYMMDD formátumban. A CCYY karakterek azt az évet jelölik, amikor a képet felvették, az MM karakterek a hónap tízes és egyes helyiértékeit, a DD karakterek pedig a hónap napjának tízes és egyes helyiértékeit. Így például 20000229 2000. február 29-ét jelöli. A teljes dátumnak egy érvényes dátumnak kell lennie.

8.1.6 15.006 mező: vízszintes sorhosszúság (HLL)

Ez a kötelező ASCII mező jelöli az átadott kép egyetlen vízszintes sorában lévő pixelek számát.

8.1.7 15.007 mező: függőleges sorhosszúság (VLL)

Ez a kötelező ASCII mező jelöli az átadott képben lévő vízszintes sorok számát.

8.1.8. 15.008 mező: skálaegységek (SLC)

Ez a kötelező ASCII mező jelöli a képfeldolgozási frekvencia (pixelsűrűség) leírására használt egységeket. A mezőben lévő „1”-es a pixel/inch, a „2”-es pedig a pixel/cm. A „0” azt jelöli, hogy nincs megadva skála. Ebben az esetben a HPS/VPS hányados adja meg a pixel-oldalarányt.

8.1.9 15.009 mező: vízszintes pixelskála (HPS)

Ez a kötelező ASCII mező jelöli a vízszintes irányban használt egészszámú pixelsűrűséget, feltéve, hogy az SLC tartalma „1” vagy „2”. Ellenkező esetben a pixel-oldalarány vízszintes komponensét jelöli.

8.1.10 15.010 mező: függőleges pixelskála (VPS)

Ez a kötelező ASCII mező jelöli a függőleges irányban használt egészszámú pixelsűrűséget, feltéve, hogy az SLC tartalma „1” vagy „2”. Ellenkező esetben a pixel-oldalarány függőleges komponensét jelöli.

9. táblázat: a 15. típusú változó felbontású tenyérnyomat-rekord felépítése

Azonosító	Kondíciós kód	Mezőszám	Mezőnév	Karaktertípus	Mezőméret előfordulásonként		Előfordulások száma		Bájtok maximális száma
					min.	max.	min.	max.	
LEN	M	15.001	LOGIKAI REKORD HOSSZA	N	4	8	1	1	15
IDC	M	15.002	KÉPKIJELÖLÉSI KARAKTER	N	2	5	1	1	12
IMP	M	15.003	LENYOMATTÍPUS	N	2	2	1	1	9
SRC	M	15.004	FORRÁSSZERVEZET/ ORI	AN	6	35	1	1	42
PCD	M	15.005	TENYÉRNYOMAT FELVÉTELÉNEK DÁTUMA	N	9	9	1	1	16
HLL	M	15.006	VÍZSZINTES SORHOSSZÚSÁG	N	4	5	1	1	12
VLL	M	15.007	FÜGGŐLEGES SORHOSSZÚSÁG	N	4	5	1	1	12
SLC	M	15.008	SKÁLAEGYSÉGEK	N	2	2	1	1	9
HPS	M	15.009	VÍZSZINTES PIXELSKÁLA	N	2	5	1	1	12
VPS	M	15.010	FÜGGŐLEGES PIXELSKÁLA	N	2	5	1	1	12
CGA	M	15.011	TÖMÖRÍTÉSI ALGORITMUS	AN	5	7	1	1	14
BPX	M	15.012	BIT/PIXEL	N	2	3	1	1	10
PLP	M	15.013	TENYÉRNYOMAT-POZÍCIÓ	N	2	3	1	1	10
RSV		15.014 15.019	FENNTARTVA KÉSŐBBI DEFINIÁLÁSRA	--	--	--	--	--	--
COM	O	15.020	KOMMENTÁR	AN	2	128	0	1	128
RSV		15.021 15.199	FENNTARTVA KÉSŐBBI DEFINIÁLÁSRA	--	--	--	--	--	--
UDF	O	15.200 15.998	FELHASZNÁLÓ ÁLTAL DEFINIÁLT MEZŐK	--	--	--	--	--	--
DAT	M	15.999	KÉPADATOK	B	2	--	1	1	--

Jelmagyarázat a karaktertípushoz: N = szám; A = betű; AN = alfanumerikus; B = bináris

10. táblázat : tenyérnyomat típusa

Leírás	Kód
Live-scan tenyér	10
Nem Live-scan tenyér	11
Látens tenyérnyomat	12
Látens tenyérnyomok	13
Látens tenyérfénykép	14
Látens tenyér lift	15

8.1.11 15.011 mező: tömörítési algoritmus (CGA)

Ez a kötelező ASCII mező jelöli a szürkeskálás képek tömörítésére használt algoritmust. A ”NONE” kód azt jelöli, hogy a rekordban lévő adat nem tömörített. A tömörítendő képekre ez a mező a tízujjas nyomatok tömörítésére preferált módszert tartalmazza. Az érvényes tömörítési kódokat az A7.1. táblázat tartalmazza.

8.1.12 15.012 mező: bit/pixel (BPX)

Ez a kötelező ASCII mező jelöli egy pixel ábrázolásához használt bitek számát. A normális, „0” és „255” közti szürkeskálás értékekre a mező „8”-at tartalmaz. Az ebben a mezőben lévő bármely, 8-nál nagyobb vagy kisebb szám rendre csökkentett vagy megnövelt precizitású szürkeskálás pixelt jelöl.

11. táblázat: tenyérkódok, -területek és -méretek

Tenyérpozíció	Tenyérkód	Képterület (mm^2)	Szélesség (mm)	Magasság (mm)
Ismeretlen tenyér	20	28387	139.7	203.2
Teljes jobb tenyér	21	28387	139.7	203.2
Jobb írástenyér	22	5645	44.5	127.0
Teljes bal tenyér	23	28387	139.7	203.2
Bal írástenyér	24	5645	44.5	127.0
Jobb alsó tenyér	25	19516	139.7	139.7
Jobb felső tenyér	26	19516	139.7	139.7
Bal alsó tenyér	27	19516	139.7	139.7
Bal felső tenyér	28	19516	139.7	139.7
Jobb egyéb	29	28387	139.7	203.2
Bal egyéb	30	28387	139.7	203.2

8.1.13 15.013 mező: tenyérnyomat-pozíció (PLP)

Ez a kötelező, címkézett mező a tenyérnyomat-képpel egyező egy vagy több lehetséges tenyérnyomat-pozíciót tartalmazza. Az ismert, vagy legvalószínűbb tenyérnyomat-pozíciónak megfelelő decimális kódszámot a 6.3-as táblázatból kell venni, és kétkarakteres ASCII-almezőként bevinni. A 6.3 táblázat az összes lehetséges tenyérnyomat-pozícióhoz tartozó maximális képméreteket is tartalmazza.

8.1.14 15.014-019 mezők: fenntartva későbbi definiálásra (RSV)

Ezek a mezők ezen szabvány későbbi módosításaiba való beillesztésre vannak fenntartva. A jelenlegi verzióban egyik mezőt sem kell használni. Ha mégis bármelyikük jelen van, nem kell figyelembe venni.

8.1.15 15.020 mező: kommentár (COM)

Ezt az opcionális mezőt kommentár, vagy más ASCII szöveges információnak a tenyérnyomatkép-adatokhoz való beillesztésére lehet használni.

8.1.16 15.021-199 mezők: fenntartva későbbi definiálásra (RSV)

Ezek a mezők ezen szabvány későbbi módosításaiba való beillesztésre vannak fenntartva. A jelenlegi verzióban egyik mezőt sem kell használni. Ha mégis bármelyikük jelen van, nem kell figyelembe venni.

8.1.17 15.200-998 mezők: felhasználó által definiált mezők (UDF)

Ezek a mezők a felhasználó által definiálhatóak. Méretüket és tartalmukat a felhasználó határozza meg, és összhangban kell állniuk a fogadó szervezettel. Ha használják őket, ASCII szöveges információkat tartalmaznak.

8.1.18 15.999 mező: képadatok (DAT)

Ez a mező egy felvett tenyérnyomat-kép összes adatát tartalmazza. Mindig a 999-es mezőszámot kell hozzárendelni, és a rekord utolsó fizikai mezőjének kell lennie. A „15.999:”-t például egy binárisan jelölt képadat követ. Alapesetben a tömörítetlen szürkeskálás adatok minden pixelét nyolc bitre (256 szürke színárnyalatra) kell méretezni. Ha a 15.012 BPX mezőben levő érték nagyobb vagy kisebb, mint „8”, a pixel leírásához szükséges bájtok száma eltérő lesz. Tömörítés esetén a pixeladatokat a CGA mezőben meghatározott tömörítési eljárással kell tömöríteni.

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

A konzisztencia érdekében a 15.999 mező adatai után közvetlenül egy „FS” szeparátort kell használni a következő logikai rekordtól való elválasztására. A szeparátort bele kell érteni a 15. típusú rekord hosszúsági mezőjébe.

8.3 További 15. típusú, változó felbontású tenyérnyomatkép-rekordok

További 15. típusú rekordokat is be lehet tenni a fájlba. Minden további tenyérnyomat-képnél egy teljes 15. típusú logikai rekordra van szükség, az „FS” szeparátorkarakterrel együtt.

1. Függelék ASCII szeparátorkódok

ASCII	pozíció[1]	Leírás
LF	1/10	A 2.074 mezőben a hibakódokat választja el egymástól.
FS	1/12	Egy fájl logikai rekordjait választja el egymástól.
GS	1/13	Egy logikai rekord mezőit választja el egymástól.
RS	1/14	Egy rekordmező almezőit választja el egymástól.
US	1/15	A mező vagy almező egyedi információs egységeit választja el egymástól.

2. Függelék Az alfanumeriklus ellenőrzési karakter kiszámítása

A TCN-re és a TCR-re (1.09 és 1.10 mezők):

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

ahol YY és SSSSSSSS rendre az év utolsó két számjegye és a sorozatszám.

Az ellenőrzési karakter ezt követően az alábbiakban megadott táblázatból generálandó.

A CRO-ra (2.010 mező)

Az ellenőrzési karakternek megfelelő számot az alábbi képlettel kell generálni:

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

ahol YY és NNNNNN rendre az év utolsó két számjegye és a sorozatszám.

Az ellenőrzési karakter ezt követően az alábbiakban megadott táblázatból generálandó.

[1] Ez az ASCII szabványban definiált pozíció.

Ellenőrzési karakterek táblázata

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	

3. Függelék Karakterkódok

Az információcsere 7 bites ANSI kódja

ASCII karakterkészlet										
+	**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**	**{**	**|**	**}**	**~**			

4. Függelék Tranzakciós összegzés

1. típusú rekord (kötelező)

Azonosító	Mezőszám	Mezőnév	CPS/PMS	SRE	ERR
LEN	1.001	Logikai rekord hossza	M	M	M
VER	1.002	Verziószám	M	M	M
CNT	1.003	Fájltartalom	M	M	M
TOT	1.004	Tranzakciótípus	M	M	M
DAT	1.005	Dátum	M	M	M
PRY	1.006	Prioritás	M	M	M
DAI	1.007	Megcélzott szervezet	M	M	M
ORI	1.008	Forrásszervezet	M	M	M
TCN	1.009	Tranzakciós ellenőrző szám	M	M	M
TCR	1.010	Tranzakciós ellenőrzés referencia	C	M	M
NSR	1.011	Eredeti szkennelési felbontás	M	M	M
NTR	1.012	Névleges átadási felbontás	M	M	M
DOM	1.013	Doménnév	M	M	M
GMT	1.014	Greenwich-i középidő	M	M	M

A kondíciós oszlopban:
O = opcionális; M = kötelező; C = feltételes, ha a tranzakció a forrásszervezetnek adott válasz

2. típusú rekord (kötelező)

Azonosító	Mezőszám	Mezőnév	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logikai rekord hossza	M	M	M	M
IDC	2.002	Képkijelölési karakter	M	M	M	M
SYS	2.003	Rendszerinformáció	M	M	M	M
CNO	2.007	Ügyszám	-	M	C	-
SQN	2.008	Sorozatszám	-	C	C	-
MID	2.009	Látensazonosító	-	C	C	-
CRN	2.010	Bűnügyi referenciaszám	M	-	C	-
MN1	2.012	Vegyes azonosítószám	-	-	C	C
MN2	2.013	Vegyes azonosítószám	-	-	C	C
MN3	2.014	Vegyes azonosítószám	-	-	C	C
MN4	2.015	Vegyes azonosítószám	-	-	C	C
INF	2.063	További információ	O	O	O	O
RLS	2.064	Válaszlista	-	-	M	-
ERM	2.074	Státusz-/hibaüzenet mező	-	-	-	M
ENC	2.320	Jelöltek elvárt száma	M	M	-	-

A kondíciós oszlopban:
O = opcionális; M = kötelező; C = Feltételes, amennyiben az adat rendelkezésre áll.
*) = ha az adatok átvitele a nemzeti jog alapján történik (a Szerződés nem fedi)

5. Függelék 1. típusú rekord-meghatározások

A.5 táblázat: 1. típusú rekord-meghatározások

Azonosító	Kondíció	Mezőszám	Mezőnév	Karaktertípus	Példa adatra
LEN	M	1.001	Logikai rekord hossza	N	1.001:230{GS}
VER	M	1.002	Verziószám	N	1.002:0300{GS}
CNT	M	1.003	Fájl	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	Tranzakciótípus	A	1.004:CPS{GS}
DAT	M	1.005	Dátum	N	1.005:20050101{GS}
PRY	M	1.006	Prioritás	N	1.006:4{GS}
DAI	M	1.007	Megcélzott szervezet	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Forrásszervezet	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Tranzakciós ellenőrző szám	AN	1.009:0200000004F{GS}
TCR	C	1.010	Tranzakciós ellenőrzési referencia	AN	1.010:0200000004F{GS}
NSR	M	1.011	Eredeti szkennelési felbontás	AN	1.011:19.68{GS}
NTR	M	1.012	Névleges átadási felbontás	AN	1.012:19.68{GS}
DOM	M	1.013	Doménnév	AN	1.013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich-i középidő	AN	1.014:20050101125959Z

A kondíciós oszlopban: O = opcionális; M = kötelező; C = feltételes
A karaktertípus-oszlopban: A=betű, N=szám, B=bináris
1* a szervezet nevénél a megengedett karakterek: ["0..9", "A..Z", "a..z", "_", ".", " ", "-"]

6. Függelék 2. típusú rekord-meghatározások

A.6.1 táblázat: CPS- és PMS-tranzakció

Azonosító	Kondíció	Mezőszám	Mezőnév	Karaktertípus	Példa adatra
LEN	M	2.001	Logikai rekord hossza	N	2.001:909{GS}
IDC	M	2.002	Képkijelölés karakter	N	2.002:00{GS}
SYS	M	2.003	Rendszerinformáció	N	2.003:0422{GS}
CRN	M	2.010	Bűnügyi referenciaszám	AN	2.010:DE/E999999999{GS}
INF	O	2.063	További információk	1*	2.063:további információk 123{GS}
ENC	M	2.320	Jelöltek elvárt száma	N	2.320:1{GS}

A.6.2 táblázat: SRE-tranzakció

Azonosító	Kondíció	Mezőszám	Mezőnév	Karaktertípus	Példa adatra
LEN	M	2.001	Logikai rekord hossza	N	2.001:909{GS}
IDC	M	2.002	Képkijelölés karakter	N	2.002:00{GS}
SYS	M	2.003	Rendszerinformáció	N	2.003:0422{GS}
CRN	M	2.010	Bűnügyi referenciaszám	AN	2.010:NL/2222222222{GS}
MN1	C	2.012	Vegyes azonosítószám	AN	2.012:E999999999{GS}
MN2	C	2.013	Vegyes azonosítószám	AN	2.013:E999999999{GS}
MN3	C	2.014	Vegyes azonosítószám	N	2.014:0001{GS}
MN4	C	2.015	Vegyes azonosítószám	A	2.015:A{GS}
INF	O	2.063	További információk	1*	2.063: további információk 123{GS}
RLS	M	2.064	Válaszlista	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

A.6.3 táblázat: ERR-tranzakció

Azonosító	Kondíció	Mezőszám	Mezőnév	Karaktertípus	Példa adatra
LEN	M	2.001	Logikai rekord hossza	N	2.001:909{GS}
IDC	M	2.002	Képkijelölés karakter	N	2.002:00{GS}
SYS	M	2.003	Rendszerinformáció	N	2.003:0422{GS}
MN1	M	2.012	Bűnügyi referenciaszám	AN	2.012:E999999999{GS}
MN2	C	2.013	Vegyes azonosítószám	AN	2.013:E999999999{GS}
MN3	C	2.014	Vegyes azonosítószám	N	2.014:0001{GS}
MN4	C	2.015	Vegyes azonosítószám	A	2.015:A{GS}
INF	O	2.063	További információk	1*	2.063: további információk 123{GS}
ERM	M	2.074	Státusz-/hibaüzenet mező	AN	2.074: 201: IDC -1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {GS}

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

Azonosító	Kondíció	Mezőszám	Mezőnév	Karaktertípus	Példa adatra
LEN	M	2.001	Logikai rekord hossza	N	2.001:909{GS}
IDC	M	2.002	Képkijelölés karakter	N	2.002:00{GS}
SYS	M	2.003	Rendszerinformáció	N	2.003:0422{GS}
CNO	M	2.007	Ügyszám	AN	2.007:E999999999{GS}
SQN	C	2.008	Sorozatszám	N	2.008:0001{GS}
MID	C	2.009	Látens-azonosító	A	2.009:A{GS}
INF	O	2.063	További információk	1*	2.063: további információk 123{GS}
ENC	M	2.320	Jelöltek elvárt száma	N	2.320:1{GS}

A kondíciós oszlopban: O = opcionális; M = kötelező; C = feltételes
A karaktertípus-oszlopban: A=betű, N=szám, B=bináris
1* a megengedett karakterek: ["0..9", "A..Z", "a..z", "_", ".", " ", "-"]

7. Függelék Szürkeskálás tömörítési kódok

A.7.1 Tömörítési kódok

Tömörítés	Érték	Megjegyzések
Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), 1997. december 19.	WSQ	A 4., 7., 13. és 15. típusú rekordokban lévő szürkeskálás képek tömörítésére használt algoritmus. Nem használható az 500 dpi-nél nagyobb felbontásokra.
JPEG 2000 [ISO 15444 / ITU T.800]	J2K	13. és 15. típusú rekordokban lévő szürkeskálás képek veszteséges és veszteség nélküli tömörítésre használandó. Erősen ajánlott 500 dpi-nél nagyobb felbontásokra.

8. Függelék E-mail-specifikációk

A belső munkafolyamat javítása érdekében a PRUEM tranzakcióban az üzenetek tárgyát az azt küldő Fél országkódjával (CC) és a tranzakciótípussal (TOT 1.004 mező) kell kitölteni.

Formátum: CC/*tranzakciótípus*
Példa: "DE/CPS"

Az üzenet törzse lehet üres.

A kódolás/aláírás és az alkalmazott S/MIME verzió specifikációja fog e helyen következni ebben a Függelékben amint lehetséges, ezen részleteknek a DNS Technikai Munkacsoporttal való megvitatását követően.

B.2 Melléklet

Ellenőrzésre elfogadott jelöltek maximális száma

AUAR-keresés típusa	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Jelöltek maximális száma	1	10	5	5	5	5	5

Keresés típusai:

TP/TP: tíz ujj nyomata – tíz ujj nyomata
LT/TP: ujjnyomat-látens – tíz ujj nyomata
LP/PP: tenyérnyomat-látens – tenyérnyomat
TP/UL: tíz ujj nyomata – azonosítatlan ujjnyomat-látens
LT/UL: ujjnyomat-látens – azonosítatlan ujjnyomat-látens
PP/ULP: tenyérnyomat – azonosítatlan tenyérnyomat-látens
LP/ULP: tenyérnyomat-látens – azonosítatlan tenyérnyomat-látens

B.3 Melléklet

Azonosított személyek ujjnyomat-adatainak maximális napi keresési kapacitása

	BE	NL	LU	AT	FR	ES	DE
BE	-	20	20	20	20	20	20
NL	20	-	20	20	16	16	24
LU	4	4	-	20	4	4	4
AT	20	20	20	-	60	60	100
FR	144	144	144	60	-	144	144
ES	120	120	120	60	120	-	120
DE	120[1)]	120[1)]	120[1)]	100	120[1)]	120[1)]	-
	428	**428**	**444**	**280**	**300**	**364**	**412**

[1)] 2007-re becsült kapacitás: napi 60 TP/TP

B.4 Melléklet

Ujjnyomat-nyomok maximális napi keresési kapacitása

	BE	NL	LU	AT	FR	ES	DE
BE	-	6	6	6	10	2	6
NL	6	-	6	6	2	2	8
LU	1	1	-	6	1	1	1
AT	6	6	6	-	15	15	30
FR	43	43	43	15	-	43	43
ES	18	18	18	15	18	-	18
DE	40 [1)]	40 [1)]	40 [1)]	30	40 [1)]	40 [1)]	-
	114	**114**	**119**	**78**	**86**	**103**	**106**

[1)] 2007-re becsült kapacitás: napi 20 LP/TP

C Mellékletek

Gépjármű-nyilvántartási adatok automatizált keresése

C.1 Melléklet

Gépjármű-nyilvántartási adatok automatizált keresésének közös adatkészlete

1. Meghatározások

A következő fejezetben leírt adatkészlet minden eleménél jelöljük, hogy azt az elemet a Felek rendelik-e hozzá, valamint hogy az elem kötelező-e vagy opcionális, amikor a csere a Szerződés 12. Cikkében leírt célokat szolgálja.

A kötelező adatelemek és az opcionális adatelemek meghatározásai az alábbiak:

Kötelező (M):
Az adatelemet közölni kell, ha az információ rendelkezésre áll a nemzeti nyilvántartásban. Tehát **ha rendelkezésre áll**, **kötelező** átadni az információt.

Opcionális (O):
Az adatelemet közölni lehet, ha az információ rendelkezésre áll a nemzeti nyilvántartásban. Tehát **nem kötelező** átadni az információt, még ha rendelkezésre is áll.

Az adatkészlet minden eleménél (Y) jelöli azokat, amelyeket a Felek a Szerződés vonatkozásában jeleznek.

2. Gépjármű/tulajdonos/üzemeltető lekérdezés

2.1 A keresés szempontjai

A következő bekezdésekben írottak szerint az információkeresésnek két módja van:

1. Alvázszám (VIN), (opcionálisan) referenciadátum és –időpont szerint;
2. Forgalmi engedély száma, (opcionálisan gépjármű fajtája / EU kategóriakód, opcionálisan) referenciadátum és –időpont szerint; Luxemburgból forgalmi engedély szerinti keresésnél egynél több gépjármű is érkezhet válaszként.

Ezen keresési kritériumok révén egy, illetve néhány esetben több gépjárműre vonatkozó adat érkezik válaszként. Ha csak egy gépjárműre vonatkozó adatot kell adni válaszként, akkor minden elemet **egy** válaszban kell megadni. Ha egynél több gépjárművet találtak, az adott Fél maga határozhatja meg,

hogy mely elemeket küldi meg válaszként: mindegyiket, vagy csak a keresés finomítását szolgálókat (pl. adatvédelmi (mint Németországban és az Egyesült Királyságban), vagy teljesítményi okok miatt).

A keresés finomításához szükséges elemeket a 2.2.1. bekezdés írja le. A 2.2.2 bekezdésben a teljes információkészlet le van írva.

Amikor a keresés alvázszám, referenciadátum és idő szerint történik, a keresést az **egyik** vagy az **összes** résztvevő országban lehet végezni.

Amikor a keresés forgalmiengedély-szám, referenciadátum és idő szerint történik, a keresést **egy adott** országban lehet végezni.

Általában a kereséskor az akkori dátumot és időpontot használják, de lehetőség van egy múltbeli referenciadátum és –időpont használatára is. Amikor a keresést egy múltbeli referenciadátummal és –időponttal végzik, és az adott Fél nyilvántartásában nem áll rendelkezésre a korábbi információ, a jelenlegi információ is lehet a válasz, jelölve, hogy ez egy aktuális információ.

2.2 Adatkészlet

2.2.1 A megkeresés finomításához szükséges, válaszként adandó elemek

Elem	**M/O[2]**	**Megjegyzések**	**Prüm Y/N[3]**
Gépjárművekre vonatkozó adatok			
Forgalmi engedély száma	M		**Y**
Alvázszám / VIN	M		**Y**
A nyilvántartást vezető Fél	M		**Y**
Gyártmány	M	(D.1[4])pl. Ford, Opel, Renault, stb.	**Y**
Gépjármű kereskedelmi márkatípusa	M	(D.3) pl. Focus, Astra, Megane	**Y**
Gépjármű fajtája / EU kategóriakód	M	(J) segédmotor, motorbicikli, személygépjármű, stb.	**Y**

2.2.2 Teljes adatkészlet

Elem	**M/O[5]**	**Megjegyzések**	**Prüm Y/N**
A gépjármű üzemeltetőjére vonatkozó adatok		**(C.1[6])**	
Az üzemeltető (cég) neve	M	(C.1.1.) Külön mezők használandók a keresztnév(ek)re, a vezetéknévre, a címekre, stb. és a nevet nyomtatható formában is közölni kell	**Y**
Keresztnév	M	(C.1.2) Külön mezők használandók a keresztnév(ek)re és kezdőbetűkre, és a nevet nyomtatható formában is közölni kell	**Y**

[2] M = kötelező, ha rendelkezésre áll a nemzeti nyilvántartásban, O=opcionális
[3] A Felek által hozzárendelt attribútumokat Y jelöli.
[4] Harmonizált dokumentum-rövidítés, lásd a Tanács 1999/37/EK (1999. április 29.) irányelvét.
[5] M = kötelező, ha rendelkezésre áll a nemzeti nyilvántartásban, O=opcionális
[6] Harmonizált dokumentum-rövidítés, lásd a Tanács 1999/37/EK (1999. április 29.) irányelvét.

Elem	**M/O**[5]	**Megjegyzések**	**Prüm Y/N**
Cím	M	(C.1.3) Külön mezők használandók az utca, házszám, irányítószám, lakóhely stb.-re, és a címet nyomtatható formában is közölni kell	**Y**
Nem	M	Férfi, nő	**Y**
Születési dátum	M		**Y**
Jogi személyiség típusa	M	Egyéni, társaság, stb.	**Y**
Azonosítószám	O	A személyt vagy a céget egyértelműen azonosító szám.	N
A gépjármű tulajdonosára vonatkozó adatok		**(C.2)**	
Tulajdonos (cég) neve	M	(C.2.1)	**Y**
Keresztnév	M	(C.2.2)	**Y**
Cím	M	(C.2.3)	**Y**
Nem	M	Férfi, nő	**Y**
Születési dátum	M		**Y**
Jogi személyiség típusa	M	Egyéni, társaság, stb.	**Y**
Azonosítószám	O	A személyt vagy a céget egyértelműen azonosító szám.	N
Járművekre vonatkozó adatok			
Forgalmiengedély-szám	M		**Y**
Alvázszám / VIN	M		**Y**
A nyilvántartó Fél	M		**Y**
Gyártmány	M	(D.1) pl.. Ford, Opel, Renault, stb.	**Y**
A jármű kereskedelmi típusa	M	(D.3) pl. Focus, Astra, Megane	**Y**
Gépjármű fajtája / EU-kategóriakód	M	(J) segédmotorok, motorbiciklik, személygépkocsik, stb.	**Y**
Első nyilvántartásba vétel dátuma	M	(B) a gépjárműnek a világon először történt nyilvántartásba vétele	**Y**
(Jelenlegi) nyilvántartás kezdete	M	(I) gépjármű-dokumentum dátuma	**Y**
Nyilvántartás vége	M		**Y**
Állapot	M	lopott, exportált, hibaüzenet	**Y**
Állapot dátuma	M		**Y**
kW	O	(P.2)	**Y**
Kapacitás	O	(P.1)	**Y**
Rendszámtípus	O	Szokásos, ideiglenes, stb.	**Y**
Gépjármű-dokumentum 1. azonosítója	O		**Y**
Gépjármű-dokumentum 1. azonosítója. Luxemburgban két külön gépjármű-nyilvántartási dokumentum-azonosítót használnak	O	A gépjármű-dokumentumra nyomtatott második egyedi dokumentum-azonosító	**Y**
Biztosítási adatok			
Biztosítótársaság neve	O		**Y**
Biztosítás kezdete	O		**Y**
Biztosítás vége	O		**Y**
Cím	O		**Y**
Biztosítás száma	O		**Y**

C.2 Melléklet

Adatbiztonság

1. Áttekintés

Az Eucaris szoftveres alkalmazás egy olyan hálózatba köti össze a Feleket, amelyben minden Fél közvetlenül kommunikál minden más Féllel. A kommunikációhoz nincs szükség egy központi komponensre. Az alkalmazás kezelni tudja a biztonságos kommunikációt a többi Fél felé, és a Felek kapcsolódó háttérrendszereivel az XML-t használva kommunikál. A Felek közvetlenül a címzettnek megküldve váltanak üzeneteket egymással. Egy Fél adatközpontja az EU Testa II hálózatára kapcsolódik.

A hálózaton keresztül küldött XML-üzenetek rejtjelezettek. A kódolásra az SSL-t használják. A háttérrendszerbe küldött üzenetek sima szöveges XML-üzenetek, mivel feltételezhető, hogy az alkalmazás és a háttérrendszerek közti kapcsolat környezete biztonságos.

Végül van egy kliensalkalmazás, amely egy Félen belül saját vagy más Felek adatbázisában való keresésre használható. A klienseket felhasználónévvel/jelszóval, vagy egy kliens-tanúsítvánnyal lehet azonosítani. Egy felhasználóhoz kiépített kapcsolat lehet rejtjelezett, ez azonban minden Fél saját felelőssége.

2. Az üzenetváltáshoz kapcsolódó tulajdonságok

A biztonság a HTTPS és az XML aláírás kombinációján alapul. Ez a változat az XML aláírást a szervernek küldött minden üzenet esetén alkalmazza, és az üzenet küldőjét az aláírás ellenőrzésével tudja azonosítani. Az egyoldalú SSL (csak egy szervertanúsítvány) az áthaladó üzenet bizalmasságának és integritásának védelmére szolgál, és a törlési és a beillesztési támadások ellen nyújt védelmet.

Az XML aláírást többféleképpen lehet alkalmazni.

Az itt választott megközelítés szerint az XML aláírást a *Web Services Security* (WSS) részeként használják. A WSS leírja az XML aláírás használatának módját. Mivel a WSS a SOAP szabványra épül, logikus a SOAP-szabványhoz alkalmazkodni, amennyire csak lehetséges. Ez a specifikált XML üzenetekhez képest változtatást igényel a címzésben, a hibakezelésben, stb.

Az XML aláírásnak és a HTTPS-nek a szevertanúsítvánnyal történő használata egyfelől az XML aláírás, másfelől a HTTPS legjobb tulajdonságait ötvözi. Nincs szükség további intézkedésekre a törlési/újraküldési támadások ellen. A kétoldalú SSL alkalmazásához testre szabott szoftverfejlesztés helyett az XML aláírást alkalmazzák. Az XML aláírás használata közelebb van a webszolgáltatásokéhoz, mint a kétoldalú SSL, és ezért stratégiailag megfelelőbb.

3. Az üzenetváltáshoz nem kapcsolódó tulajdonságok

3.1 Felhasználók azonosítása

Az Eucaris webes alkalmazásának felhasználói felhasználónévvel és jelszóval azonosítják magukat. Mivel a szokványos Windows-os azonosításról van szó, a Felek klienstanúsítványok révén növelhetik az azonosítás szintjét, szükség esetén.

3.2 Felhasználói szerepek

Az Eucaris szoftveres alkalmazása különböző felhasználói szerepeket támogat. Minden szolgáltatáscsoportnak megvan a maga azonosítási módja. Pl. az „Eucaris-szerződés funkció” (kizárólagos) használói nem használhatják a „Prümi Szerződés funkciót”. Az adminisztrátor-szolgáltatások el vannak választva a normális végfelhasználói szerepektől.

3.3 Az üzenetváltás naplózása és nyomonkövetése

Az Eucaris szoftveres alkalmazása lehetővé teszi minden üzenettípus naplózását. Az adminisztrátor-funkció lehetővé teszi a nemzeti adminisztrátor számára, hogy meghatározza, mely üzeneteket naplózzák: a végfelhasználók kérelmeit, a más Felektől beérkező kérelmeket, a nemzeti nyilvántartásokból szolgáltatott adatokat, stb.

Az alkalmazás konfigurálható úgy, hogy ehhez a naplózáshoz egy belső vagy egy külső (Oracle) adatbázist használjon. A naplózandó üzenetekről szóló döntés nyilvánvalóan a háttérrendszerek és a csatlakozó kliensalkalmazások naplózási képességeitől függ.

Minden üzenet fejléce tartalmaz a kérelmező Félre, azon belül a kérelmező szervezetre és az érintett felhasználóra vonatkozó információt. A kérés okát is jelölik

A kérelmező és a választ adó Fél általi kombinált naplózás révén minden üzenetváltás teljesen nyomon követhető (pl. egy érintett állampolgár kérésére).

A naplózás az Eucaris webes kliensén (Adminisztrációs menü, Naplózási beállítások) keresztül van konfigurálva. A naplózási funkciót az Alaprendszer végzi. Ha a naplózás be van kapcsolva, a teljes üzenet (a fejléc és a törzs) egy naplózási rekordban lesz tárolva. A naplózási szintet meghatározott szolgáltatásonként és az alaprendszeren áthaladó üzenettípusonként lehet beállítani.

Naplózási szintek
Az alábbi naplózási szintek lehetségesek:
Privát – Az üzenet naplózva van: A naplózás NEM áll a titkársági funkciót ellátó állam által üzemeltetett kivonatos naplózási szolgáltatás rendelkezésére, hanem csak nemzeti szinten, ellenőrzések és problémamegoldás céljára hozzáférhető.
Nincs – Az üzenetet egyáltalán nem naplózzák.

Üzenettípusok

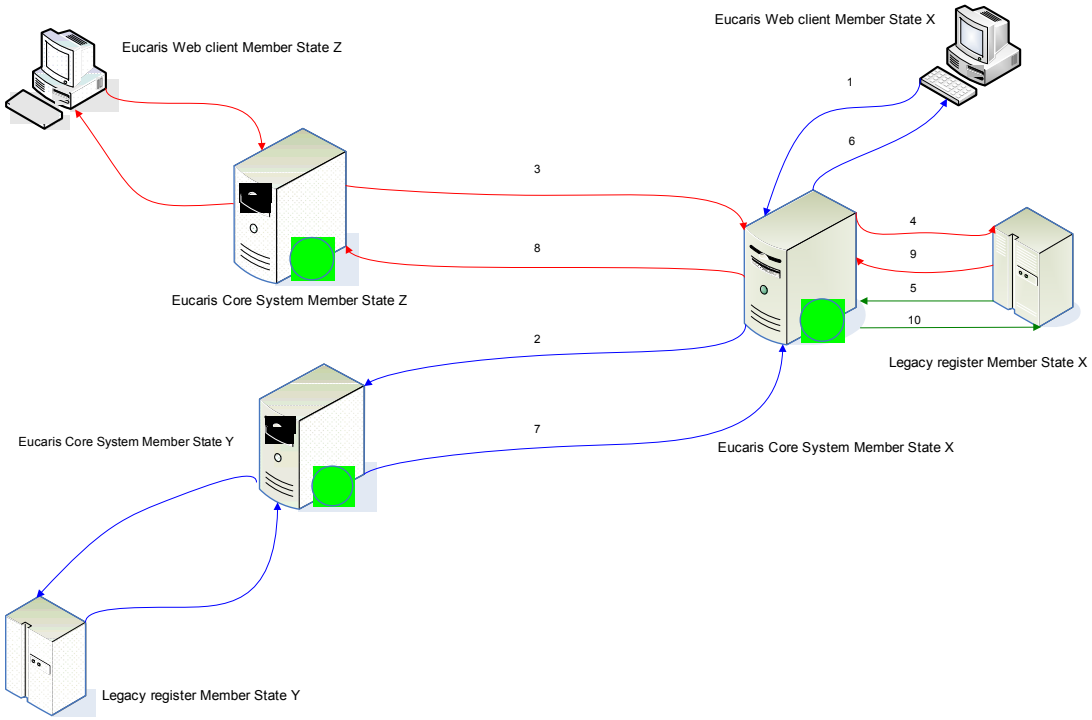
A Felek közti információcsere több üzenetből áll, amelyek sematikus ábrázolását az alábbi ábra mutatja.

A lehetséges üzenettípusok (az ábrán az X Fél Eucaris Alaprendszerére vonatkozóan) az alábbiak:

1. Kérelem az Alaprendszernek_Kérelem üzenet a kliens által
2. Kérelem másik Félnek_ Kérelem üzenet ezen Fél Alaprendszere által
3. Kérelem ezen Fél Alaprendszerének_ Kérelem üzenet más Fél Alaprendszere által
4. Kérelem a kapcsolódó nyilvántartásnak_ Kérelem üzenet az Alaprendszer által
5. Kérelem az Alaprendszernek_ Kérelem üzenet a kapcsolódó nyilvántartás által
6. Válasz az Alaprendszertől_ Kérelem üzenet a kliens által
7. Válasz másik Féltől_ Kérelem üzenet ezen Fél Alaprendszere által
8. Válasz ennek a Félnek az Alaprendszerétől _ Kérelem üzenet más Fél által
9. Válasz a kapcsolódó nyilvántartástól_Kérelem üzenet az Alaprendszer által
10. Válasz az Alaprendszertől _ Kérelem üzenet a kapcsolódó nyilvántartás által

Az alábbi információcserék láthatóak az ábrán:

- Információkérés e Fél (X) által egy másik Féltől (Y) – kék nyilak. Ez a kérelem és válasz rendre 1., 2., 7. és 6. típusú üzenetekből áll.
- Információkérés egy másik Fél (Z) által ettől a Féltől (X) – piros nyilak. Ez a kérelem és válasz rendre 3., 4., 9. és 8. típusú üzenetekből áll.
- Információkérés a kapcsolódó nyilvántartás által az alaprendszerétől (ez az út tartalmazza a kapcsolódó nyilvántartás mögötti kliens kérelmét is) – zöld nyilak. Ez a fajta kérelem 5. és 10. típusú üzenetekből áll.



Ábra : Naplózási üzenettípusok

3.4 Hardverbiztonsági modul

Hardverbiztonsági modul nem használatos.

Egy hardverbiztonsági modul (HSM) az üzenetek aláírására szolgáló kulcs védelmének és a szerverek azonosításának megfelelő eszköze. Ez növeli a biztonság szintjét, de a HSM-et igen költséges beszerezni és fenntartani, és nem követelmény a FIPS 140-2 2. vagy 3. szintű HSM alkalmazása. Mivel a Felek zárt hálózatot használnak, amelyik hatékonyan enyhíti a fenyegetettséget, úgy döntöttek, hogy kezdetben nem alkalmaznak HSM-et. Ha mégis szükséges egy HSM, pl. a tanúsítvány beszerzéséhez, hozzá lehet adni az architektúrához.

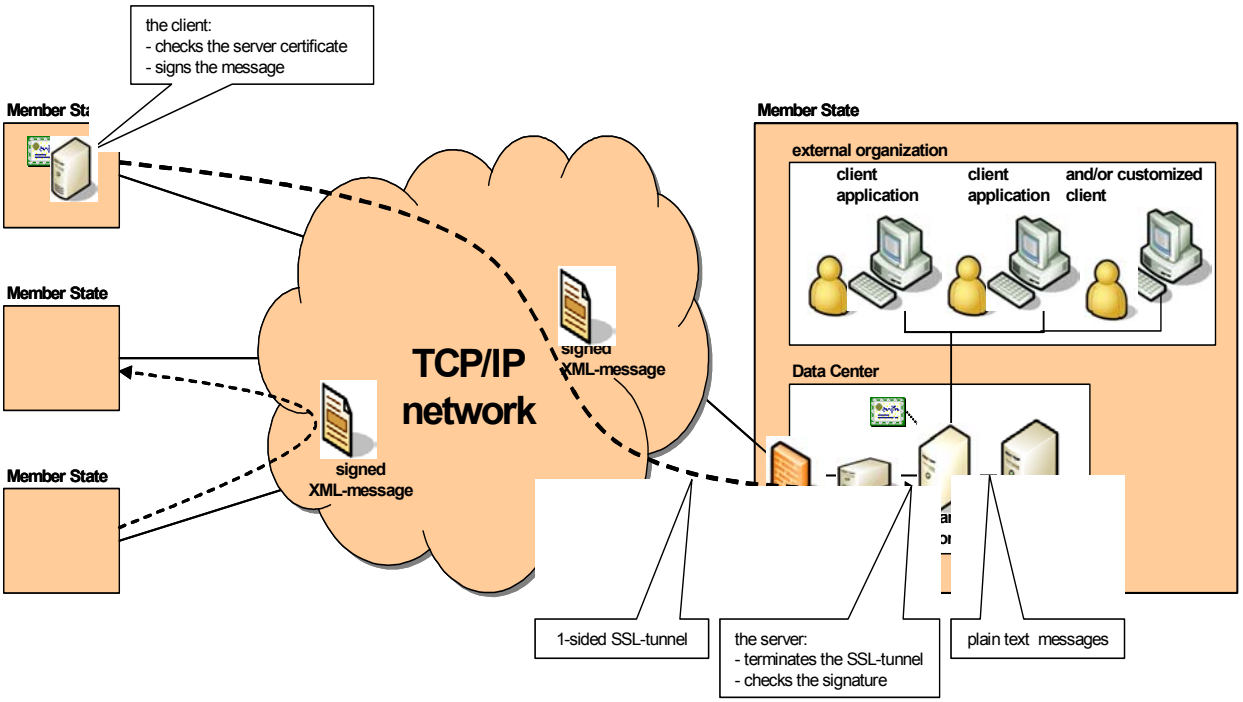
C.3 Melléklet

Az adatcsere műszaki feltételei

1. Az EUCARIS alkalmazás általános leírása

1.1 Áttekintés

Az Eucaris szoftveres alkalmazás egy olyan hálózatba köti össze a Feleket, amelyben minden Fél közvetlenül kommunikál minden Féllel. A kommunikációhoz nincs szükség egy központi komponensre. Az alkalmazás kezelni tudja a biztonságos kommunikációt a többi Fél felé, és a Felek kapcsolódó háttérrendszereivel az XML-t használva kommunikál. Az alábbi kép szemlélteti ezt az architektúrát.



A Felek közvetlenül a címzettnek küldve váltanak üzenetet egymással. Egy Fél adatközpontja a üzenetcserére használt hálózatra (Testa) van kapcsolva. A Testa hálózathoz való hozzáféréshez a Felek nemzeti összeköttetési pontjukon keresztül kapcsolódnak. Alapesetben a hálózathoz való kapcsolódásnál tűzfalat használnak, és egy router köti össze az Eucaris alkalmazást a tűzfallal. Az üzenetek védelmére választott módszertől függően a tanúsítványt vagy a router, vagy az Eucaris alkalmazás használja.

A hálózaton keresztül küldött XML-üzenetek rejtjelezettek. A kódolásra az SSL-ta használják. A háttérrendszerbe küldött üzenetek sima szöveges XML-üzenetek, mivel feltételezhető, hogy az alkalmazás és a háttérrendszerek közti kapcsolat környezete biztonságos.

Végül van egy kliensalkalmazás, amely egy Félen belül saját vagy más Felek adatbázisában való keresésre használható. A kliensalkalmazás az Eucarishoz kapcsolódik. A klienseket felhasználónévvel/jelszóval, vagy egy kliens-tanúsítvánnyal lehet azonosítani. Egy felhasználóhoz (pl. a rendőrséghez) kiépített kapcsolat lehet rejtjelezett, ez azonban minden Fél saját felelőssége.

1.2 A rendszer hatóköre

Az Eucaris rendszer hatóköre a Felek nyilvántartási hatóságai közti információcserére és ennek az információnak a bemutatására korlátozódik. Az eljárások és automatizált folyamatok, amelyekben az információ használandó (pl. adminisztratív, vagy rendészeti lépések) a rendszer hatókörén kívül esnek.

A Felek választhatnak, hogy az Eucaris kliensfunkcióját, vagy saját testreszabott kliensalkalmazásukat használják-e. Az alábbi táblázatban le van írva, hogy az Eucaris rendszer mely elemei kötelezőek és/vagy adottak, és melyek opcionálisak, és/vagy a Felek által szabadon meghatározhatóak.

EUCARIS-elemek	M/O[7]	Megjegyzés
Hálózati koncepció	M	A koncepció a „bármely két fél közti” kommunikáció
Fizikai hálózat	M	TESTA
Alapalkalmazás	M	Az EUCARIS alapalkalmazását a többi Félhez való csatlakozásra kell használni. Az alapalkalmazás az alábbi funkciókat kínálja: ▪ Üzenetek rejtjelezése és aláírása; ▪ Küldő azonosságának ellenőrzése; ▪ Felek és helyi felhasználók engedélyezése; ▪ Üzenetek továbbítása; ▪ Aszinkron üzenetek várakoztatása, ha a fogadó szolgáltatás ideiglenesen nem elérhető; ▪ Többszörös ország-lekérdezési funkció; ▪ Az üzenetek naplózása; ▪ A bejövő üzenetek tárolása
Kliens-alkalmazás	O	Az alapalkalmazás mellett az EUCARIS II kliens-alkalmazást is használhatja egy Fél. Igény esetén az alap- és a kliensalkalmazást az EUCARIS szervezet felügyelete mellett módosítani lehet.

[7] M = kötelező használni, vagy ennek megfelelni O = használata vagy a megfelelés opcionális

EUCARIS-elemek	M/O[7]	Megjegyzés
Biztonsági koncepció	M	A koncepció klienstanúsítványokon alapuló XML-aláíráson és szolgáltatói tanúsítványokon alapuló SSL-kódoláson alapul.
Üzenet-specifikációk	M	Minden Félnek meg kell felelnie az EUCARIS szervezet és a jelen Végrehajtási Megállapodás, illetve ennek C Mellékletei által rögzített üzenet-specifikációknak. A specifikációkat csak az EUCARIS szervezet változtathatja meg, a Felekkel konzultálva.
Működés és segítségnyújtás	M	Az EUCARIS szervezet dönt új Felek, vagy új funkciók elfogadásáról. A monitoring, illetve segítségnyújtási feladatokat egy kijelölt Fél központilag végzi.

2. Nem-funkcionális követelmények

2.1 Alapvető funkciók

Ebben a szakaszban a legfontosabb alapvető funkciókat írjuk le, általánosságban.

Szám	Leírás
1.	A rendszer lehetővé teszi a Felek nyilvántartási hatóságai számára a kérelmező és válaszüzenetek interaktív módon történő cseréjét.
2.	A rendszer egy kliensalkalmazást tartalmaz, amely lehetővé teszi a végfelhasználók számára, hogy elküldjék kérelmeiket, és hogy kézi feldolgozásra átadják a válaszinformációkat.
3.	A rendszer megkönnyíti a „szórást”, lehetővé téve az egyik Fél számára, hogy kérelmét az összes többi Félnek eljuttassa. A bejövő válaszokat az alapalkalmazás összegzi egy válaszüzenetben a kliensalkalmazás számára (ezt a funkciót ’Többszörös országlekérdezésnek’ nevezik).
4.	A rendszer képes különböző típusú információk kezelésére. A felhasználói szerepeket, engedélyezést, továbbítást, aláírást, naplózást mind-mind az adott szolgáltató határozza meg.
5.	A rendszer lehetővé teszi a Felek számára üzenetcsomagok, vagy nagyszámú kérelmet, vagy választ tartalmazó üzenetek cseréjét. Ezeket az üzeneteket aszinkron módon kezeli.
6.	A rendszer várakoztatja az aszinkron üzeneteket, ha a fogadó Fél átmenetileg nem elérhető, és garantálja kézbesítéseket, amint a fogadó újra készen áll.
7.	A rendszer tárolja a bejövő aszinkron üzeneteket, amíg azokat fel nem lehet dolgozni.
8.	A rendszer csak más Felek Eucaris-alkalmazásainak ad hozzáférést, ezen Felek egyes szervezeteinek nem, azaz minden nyilvántartási hatóság egyetlen összeköttetési pontként szolgál saját nemzeti végfelhasználói és a többi Fél megfelelő hatóságai közt.
9.	Lehetőség van egy Eucaris-szerver különböző Felei felhasználóinak definiálására, és az adott Fél által élvezett jogokkal való felruházásukra.
10.	A kérelmező Félre, szervezetre és végfelhasználóra vonatkozó információk benne vannak az üzenetben.
11.	A rendszer megkönnyíti a Felek közti, illetve az alapalkalmazás és a nemzeti nyilvántartási rendszerek közti üzenetváltás naplózását.
12.	A rendszer lehetővé teszi egy adott titkár (amely egy erre a feladatra külön kijelölt szervezet vagy Fél lehet) számára, hogy begyűjtse az összes résztvevő Fél által

Szám	Leírás
	elküldött/fogadott üzenetekre vonatkozó, naplózott információkat, statisztikai jelentések készítése céljából.
13.	Minden Fél maga jelzi, hogy a titkár számára milyen naplózott információkat tesz elérhetővé, illetve melyeket minősíti ’privátnak’.
14.	A rendszer lehetővé teszi minden Fél nemzeti adminisztrátora számára, hogy statisztikákat készítsen a használatról.
15.	A rendszer lehetővé teszi további Felek hozzáadását egyszerű adminisztratív lépésekkel.

2.2 Használhatóság

Szám.	Leírása
16.	A rendszer egy felületet biztosít az üzenetek hátsó rendszerek általi automatizált feldolgozására, és lehetővé teszi a felhasználói felület integrálását ezekbe a rendszerekbe (testreszabott felhasználói interfész)
17.	A rendszert könnyű megtanulni, magától értetődő, és súgót is tartalmaz.
18.	A rendszer dokumentált, ami segíti a Feleket az integrálásában, az operatív teendőkben és a későbbi fenntartásban (pl. használati útmutatók, funkcionális/műszaki dokumentáció, operatív iránymutató,…).
19.	A felhasználói felület többnyelvű, és lehetővé teszi a végfelhasználó számára, hogy az általa előnyben részesített nyelvet válassza.
20.	A felhasználói felület lehetővé teszi a helyi adminisztrátor számára, hogy mind a képernyőn megjelenő elemeket, mind a kódolt információt saját nyelvére fordítsa.

2.3 Megbízhatóság

Szám.	Leírás
21.	A rendszer robusztus és megbízható operációs rendszer, amely ellenáll az operátor által elkövetett hibáknak, és áramkimaradás vagy egyéb káresemény után újraindítható. Adatveszteség nélkül, vagy minimális adatveszteséggel újraindíthatónak kell lennie.
22.	A rendszernek stabil és reprodukálható eredményeket kell adnia.
23.	A rendszert úgy tervezték, hogy megbízhatóan működjön. Lehetőség van a rendszert olyan konfigurációban telepíteni, amelyik 98 százalékos rendelkezésre állást garantál (redundanciával, támogató szerverek használatával, stb.) minden kétoldalú kommunikáció esetében.
24.	Lehetőség van a rendszer egy részének használatára, néhány összetevőjének meghibásodása esetén is (ha a C Fél nem működik, A és B attól még tud egymással kommunikálni). Az információs láncban az egyedi meghibásodható pontok számát minimalizálni kell.
25.	Egy súlyos meghibásodást követő helyreállítás idejének egy napnál rövidebbnek kell lennie. Lehetséges kell, hogy legyen a nem-működési időtartamnak egy távoli támogatással (pl. központi szervízállomással) történő minimalizálása.

2.4 Teljesítmény

Szám	Leírás
26.	A rendszert a hét minden napján, napi 24 órában lehet használni. Ezt az időkeretet a Felek csatlakozó rendszereitől is elvárják.
27.	A rendszer gyorsan válaszol a felhasználói megkeresésekre, tekintet nélkül a háttérfeladatokra. Ezt a Felek csatlakozó rendszereitől is elvárják az elfogadható válaszadási idő biztosítása érdekében. Egyetlen kérésénél legfeljebb 10 másodperc lehet a teljes válaszadási idő.
28.	A rendszert többfelhasználósnak tervezték, és oly módon, hogy a háttérfeladatok folytatódhassanak, amíg a felhasználó az előtérben lévő feladatokat végzi.
29.	A rendszert skálázhatónak tervezték, hogy új funkciók vagy szervezetek, illetve Felek hozzáadásakor az üzenetek számának esetleges növelését elviselje.

2.5 Biztonság

Szám	Leírás
30.	A rendszer megfelelő (pl. biztonsági intézkedései tekintetében) az adatvédelmi szempontból kényes, „EU korlátozott terjesztésű” minősítéssel ellátott személyes adatokat (pl. járműtulajdonos/üzemeltető, jogosítvány-tulajdonos) tartalmazó üzenetek váltására
31.	A rendszer fenntartása megakadályozza az adatokhoz való jogosulatlan hozzáférést. .
32.	A rendszer a nemzeti végfelhasználók jogainak és engedélyeinek kezelésére való szolgáltatást is tartalmaz.
33.	A Felek az XML-aláírás révén azonosítani tudják a küldő azonosságát (a Fél szintjén).
34.	A Feleknek kifejezetten engedélyezniük kell más Fél számára konkrét információ kérését, lehetővé téve az információcserét egy konkrét szerződés vagy irányelv hatályán belül és kívül egyaránt.
35.	A rendszer az alkalmazás szintjén egy teljes biztonsági és rejtjelezési eljárást nyújt, amely megfelel az adott helyzetben előírt biztonsági szintnek. Az információk kizárólagosságát és integritását az XML-aláírás és az SSL-csatornázás révén történő rejtjelezés garantálja.
36.	Minden üzenetváltás nyomon követhető a naplózás révén.
37.	A rendszer védelmet nyújt a törlési kísérletek (egy harmadik fél töröl egy üzenetet), az újraküldési vagy beillesztési támadások (egy harmadik fél újraküld, vagy beilleszt egy üzenetet) ellen.
38.	A rendszer egy Megbízható Harmadik Fél (*Trusted Third Party* – TTP) által kiállított tanúsítványokat használ.
39.	A rendszer képes egy Félnél több különböző tanúsítvány kezelésére is, az üzenet vagy a szolgáltatás típusától függően.
40.	Az alkalmazási szintű biztonsági intézkedések elegendőek a nem-akkreditált hálózatok használatának lehetővé tételéhez is.
41.	A rendszer képes az új biztonságtechnikák, mint például az XML-tűzfal használatára is.

2.6 Adaptálhatóság

Szám	Leírás
42.	A rendszert ki lehet bővíteni új üzenetekkel és új funkciókkal (pl. névpárosítási algoritmusok). Az adaptálás költségei minimálisak, az alkalmazási összetevők központosított fejlesztésének köszönhetően.
43.	A tagállamok kétoldalú használatra új üzenettípusokat definiálhatnak. Nincs előírva, hogy minden Fél minden üzenettípust támogasson.

2.7 Segítségnyújtás és fenntartás

Szám	Leírás
44.	A rendszer egy központi szerviz és/vagy operátorok számára biztosítja az egyes Felek hálózatainak és szervereinek monitoringját.
45.	A rendszer biztosítja egy központi szervíz által távolról nyújtott támogatás eszközeit.
46.	A rendszer biztosítja a problémaelemzés eszközeit.
47.	A rendszert ki lehet terjeszteni további Felekre.
48.	Az alkalmazást könnyű telepíteni.
49.	A rendszer állandó teszt- és elfogadási környezetet biztosít.
50.	A segítségnyújtás és a fenntartás éves költségeit minimalizálták, a kereskedelmi szabványok alkalmazásával és azzal, hogy az alkalmazást úgy alkották meg, hogy minél kisebb szükség legyen egy központi szerviz támogatására.

2.8 Tervezési követelmények

Szám	Leírás
51.	A rendszert több éves élettartamúra tervezték és dokumentálták.
52.	A rendszert a hálózati szolgáltatótól függetlennek tervezték.
53.	A rendszer megfelel a Feleknél meglévő hardvereknek és szoftvereknek, ezekkel a nyilvántartási rendszerekkel a szokványos webes technológia (XML, HTTP, webszolgáltatások, WSS) használatával kommunikál.

2.9 Alkalmazható szabványok

Szám	Leírás
54.	A rendszer megfelel a 45/2001/EK rendelet 21., 22. és 23. Cikkének, valamint a 95/46/EK irányelvnek.
55.	A rendszer megfelel az IDA-szabványoknak [doc-1].
56.	A rendszer támogatja az UTF8-at.

C.4 Melléklet

A bejövő kérések kapcsolattartó pontjainak listája

Ország	Kapcsolattartó pont	Telefonszám (operatív kapcsolatteremtés céljára)	Faxszám (operatív kapcsolatteremtés céljára)	E-mail cím (operatív kapcsolatteremtés céljára)
Ausztria	Bundeskriminalamt Österreich (Osztrák Bűnügyi Hírszerzési Szolgálat))	**+43 1 24836 85026**	**+43 1 24836 951135**	**BMI-II-BK-SPOC@bmi.gv.at**
Belgium	DIV „Dienst Inschrijvingen” (Gépjármű-nyilvántartás)	**+ 32 2 2773 792 (DIV)** **+ 32 2 2773 777 (ICT)**	**+ 32 2 277 40 22 (DIV)** **+ 32 2 277 40 04**	**Help.div@mobilit.fgov.be (DIV)** **Help.ict@mobilit.fgov.be (ICT)**
Franciaország	SCCOPOL „Section Centrale de Coopération policière” (Bűnügyi nyomozó rendőrség)	**+ 33 (0) 1 40 97 88 73**	**+ 33 (0) 1 40 97 82 48**	**dcpj-dri-pcc@interieur.gouv.fr**
Németország	KBA „Kraftfahrt-Bundesamt” (Gépjármű-nyilvántartás)	**+ 49 461 316 2050**	**+ 49 461 316 2942**	**pruem@kba.de**
Luxemburg	Centre Informatique de la Police (Rendőrség)	**+ 35 2 4997 2346**	**+ 35 2 4997 2398**	**cin@police.etat.lu**
Hollandia	RDW „Rijksdienst Wegverkeer” (Gépjármű-nyilvántartás)	**+ 31 598 693 369**	**+ 31 503 656 462**	**servicedesk@rdw.nl**
Spanyolország	Secretaria de Estado de Seguridad (Belügyminisztérium)	**+34915371883** **+34915371884** **+34915372056** **+34915372057** **+34915372058**	**+34913191228** **+34913191645** **+34913197389**	**cepic@ses.mir.es**

D Mellékletek

Rendőri együttműködés

D.1 Melléklet

Közös műveletek indítására szolgáló eljárások és kapcsolattartó pontok

Azok a Felek, amelyek nem használnak olyan meghatározott eljárásokat (illetve nem dolgoznak ilyenekkel), amelyeknél egy kapcsolattartó pont közreműködésére van szükség a Szerződés 24. Cikke szerinti közös műveletek elindításához, az alábbi kapcsolattartó pontokat adják meg a közös műveletek elindításához.

AUSZTRIA

A Végrehajtási megállapodás 14.2 pontja szerinti nemzeti kapcsolattartó pont:

Munkaidőben:
Szövetségi Belügyminisztérium, Közbiztonsági Főigazgatóság,
II/2/a alosztály
Telefon: +431-53126-3411
Fax: +431-53126-10-8638
E-mail: bmi-II-2-a@bmi.gv.at

Munkaidőn kívül:
Szövetségi Belügyminisztérium, II. Divízió – Közbiztonsági Főigazgatóság, Műveleti és Válságkoordinációs Központ
Telefon: +431-53126-3200 vagy -3775
Fax: +431-53126-3120
E-mail: bmi-II-EKC-Permanenzdienst@bmi.gv.at

BELGIUM

1. Közös őrjáratok és közös ellenőrzések

Nincs követendő formális eljárás közös őrjárat vagy közös ellenőrzés indításakor. Elegendő, hogy az érintett szolgálatok operatív vezetői (Belgiumban: a helyi rendőrség testületi parancsnoka, vagy a szövetségi rendőrség egységparancsnoka) szóban vagy írásban megállapodjanak. Ha valaki nem tudja, hogyan lépjen kapcsolatba a belgiumi operatív vezetéssel, a nemzeti kapcsolattartó pontot keresse meg:

DAO (Adminisztratív rendőrségi operatív igazgatóság – ügyeletes tiszt)
Blok G, Fritz Toussaintstraat 47
1050 Elsene
Tel.: + 32 2 642.63.80
Fax: + 32 2 646.49.40
E-mail: dga-dao@skynet.be.

Az operatív vezetők biztosítják, hogy a műveletben részt vevő minden tiszt tájékoztatást kapjon a feladatról és a kompetenciákról. Szükség esetén egy megbeszélést tartanak e célból.

2. Egyéb közös műveletek

Egyéb közös műveletekre csak megkeresés alapján van lehetőség. A Belga Rendőrségnek címzett megkeresést az alábbi űrlapot kitöltve a nemzeti kapcsolattartó pontnak kell küldeni:

DAO (Adminisztratív rendőrségi operatív igazgatóság – ügyeletes tiszt)
Blok G, Fritz Toussaintstraat 47
1050 Elsene
Tel.: + 32 2 642.63.80
Fax: + 32 2 646.49.40
E-mail: dga-dao@skynet.be.

A kompetens belga hatóság azonnali döntést hoz a megkeresésről. A döntést a megkereső Fél kompetens hatóságának a lehető leggyorsabban, írásban küldik meg.

A közös műveletek végrehajtása során a határt átlépő tisztnél a magával hozott eszközökről és anyagokról egy összesítő lista található. Ezt kérésre a fogadó ország kompetens hatóságának adja át.

FRANCIAORSZÁG

	Szervezet	Település	Telefonszám Faxszám E-mail
AUSZTRIA	CCPD	Kehl	Tel : 0049.7851.8895-0 Fax : 03 90 23 13 69 E-mail: centro.lz@1.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr vagy : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)

	Szervezet	Település	Telefonszám Faxszám E-mail
HOLLANDIA	CCPD	Tournai	Tel : 00 32 69 68 26 10 Fax :00 32 69 68 26 21 E-mail : ccpd-tournai.dzaf-59@interieur.gouv.fr
NÉMETORSZÁG	CCPD	Kehl	Tel : 0049.7851.8895-0 Fax : 03 90 23 13 69 E-mail: centro.lz@1.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr vagy : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)
SPANYOLORSZÁG	CCPD	Hendaye	Tel : 05 59 20 93 60 Fax: 05 59 20 59 34 E-mail : ccpd-hendaye@interieur.gouv.fr
	CCPD	Le Perthus	Tel : 04 68 83 79 00 Fax : O4 68 83 79 10 Tel : 05 59 20 93 60 Fax : 05 59 20 59 34 E-mail : ccpd-hendaye@interieur.gouv.frccpd-sec.le-perthus-66@intermel.si.mi
	CCPD	Canfranc le Somport	Tel : 05 59 39 04 85 Fax : 05 59 36 18 15 E-mail : ccpd.canfranc@interieur.gouv.fr
	CCPD	Melles Pont du Roy	Tel : 05 61 94 68 40 Fax : 05 61 94 68 48 E-mail : ccpd.melles@interieur.gouv.fr
BELGIUM	CCPD	Tournai	Tel : 00 32 69 68 26 10 Fax :00 32 69 68 26 21 E-mail : ccpd-tournai.dzaf-59@interieur.gouv.fr

	Szervezet	Település	Telefonszám Faxszám E-mail
LUXEMBURG	CCPD	Luxembourg	Tel : 03 82 54 94 30 vagy +352 26 124 300 Fax : 03 82 54 94 39 vagy +352 26 124 199 E-mail : fr@bccp.etat.lu

NÉMETORSZÁG

1. Bevezetés a 24. Cikkhez

Általánosságban minden tartományi és szövetségi rendőrkapitányság felelős lehet közös műveletekért.

Ez azonban csak akkor van így,
- ha a közös műveleteket szabályozó két- és többoldalú szerződések nem tartalmaznak konkrétabb szabályozást, és
- ha a közös műveleteknek nincs közvetlen határokon átnyúló kapcsolódása (pl. spanyol rendőrök Németországban).

Ha a közös műveletek tekintetében nincs konkrétabb szerződéses rendelkezés hatályban, és nincs közvetlen határon átnyúló kapcsolódás, ezek a kivételes esetek a szövetségi Belügyminisztérium és/vagy az érintett tartományi belügyminisztériumok beleegyezését igénylik.

A 24. Cikk (1) és (2) bekezdése elválaszthatatlanul kapcsolódik egymáshoz. Az (1) bekezdés szerinti minden **intézkedéshez** a **beleegyezést** ugyanúgy be kell szerezni a szuverén jogok átruházásáról, az operatív feltételekről és a fogadó ország tisztjeinek jogkörében maradó műveleti irányításról szóló (2) bekezdéshez.

2. A 24. Cikk (1) bekezdéshez – „a Szerződő Felek által kijelölt hatóságok”

Példák közös műveletekre:

Főként „nem időkritikus helyzetek” (a tervezett események előkészítése során – „*Zeitlagen*”), mint a határrégióban végzett közös őrjáratok, különleges események (pl. Alsószászok Napja) alkalmából folytatott közös őrjáratok, közös ellenőrzések (pl. a nemzetközi bűnözés – kábítószer-bűncselekmények, emberkereskedelem, csoportosan elkövetett, tulajdon elleni bűncselekmények (más néven „konkrét gyanúsítástól független” ellenőrzések), közös bűnügyi hírszerzési intézkedések / potenciális elkövetőkre való figyelmeztetés / szurkolók kísérete labdarúgó-mérkőzések vagy más jelentős események során.

Az 1. pontban említett alapelvek alkalmazandóak.

Általános kapcsolattartó pontok, más Szerződő Felek részére is:	
(közvetlen, határon átnyúló együttműködés)	
Bundespolizei Bundespolizeidirektion Roonstr. 13 D-56068 Koblenz	Tel.: +49 (0) 261 399 – 0 Tel.: +49 (0) 261 399 – 250 Fax.: +49 (0) 261 399 – 218 Mail: bpold@polizei.bund.de

3. A 24. cikk (2) bekezdés 1. mondatához – "beleegyezés szuverén jogok gyakorlásába"

A Szövetségi Belügyminisztérium beleegyezését igénylő együttműködések:

Szövetségi Belügyminisztérium (Bundesministerium des Innern)
- Szövetségi Bűnügyi Hivatal (Bundeskriminalamt):
  Rendőri és Terrorizmus Elleni Küzdelem Főosztálya (*Abteilung Polizeiangelegenheiten; Terrorismusbekämpfung*)
- Szövetségi Rendőrség (*Bundespolizei*):
  Szövetségi Rendőrségi Főosztály (*Abteilung für Angelegenheiten der Bundespolizei*)

Alt-Moabit 101D
D-10559 Berlin

Tel.: +49 (0) 1888 681-1077
Fax.: +49 (0) 1888 681-2926
E-mail: poststelle@bmi.bund.de

Tel.: +49 (0) 1888 681-0
Fax: +49 (0) 1888 681-1829
E-mail: poststelle@bmi.bund.de

Tartományi belügyminisztériumi beleegyezést igénylő együttműködések. Az alábbiakban a többi prümi Szerződő Féllel határos tartományok találhatóak.

Alsószászország (NI)
Niedersächsisches Ministerium für Inneres und Sport
Lavesallee 6
D-30169 Hannover

Tel.: +49 (0) 511 120-6112
Fax.: +49 (0) 511 120-6150
Mail: kvl@mi.niedersachsen.de

Észak-Rajna-Vesztfália (NW)
Innenministerium Nordrhein-Westfalen
- Lagezentrum –
Haroldstraße 5
40190 Düsseldorf

Tel.: +49 (0)211 871 3340/3341/3342/3343/3344
Fax.: +49 (0)211 871 3231
Mail: lagezentrum@im.nrw.de

Rheinland-Pfalz (RP) Ministerium des Innern und für Sport - Lagezentrum - Schillerplatz 3-5 55116 Mainz	Tel.: +49 (0)6131 16 3599 Fax.: +49 (0)6131 16 3600 Mail: lagezentrum@ism.rlp.de
Saarland (SL) Ministerium für Inneres, Familie, Frauen und Sport Leitstelle, Lagezentrum- c/o Landespolizeidirektion Mainzer Str 134 -136 66121 Saarbrücken	Tel.: +49 (0) 681 962-1260 bis 1263 Fax.: +49 (0) 681 962-1265 Mail: lagezentrum@innensaarland.de
Baden-Württemberg (BW) Innenministerium Baden-Württemberg Lagezentrum Dorotheenstraße 6 70173 Stuttgart	Tel.: +49 (0)711 231 3333 Fax.: +49 (0)711 231 3399 Mail: lagezentrum@im.bwl.de
Bajorország (BY) Bayerisches Staatsministerium des Innern - Lagezentrum - Odeonsplatz 3 D-80335 München	Tel.: 0049 (0) 89 2192-20 Fax: 0049 (0) 89 2192-2587 Mail: stmi.lzby@polizei.bayern.de

Egyetlen prümi szerződő Féllel sem határos tartományok:

Brandenburg (BB) Ministerium des Innern des Landes Brandenburg Lageszentrum der Polizei Henning-von-Treskow-Str. 9-13 14467 Potsdam	Tel.: +49 331 866 2871 Fax.: +49 331 866 2879 Mail: lagezentrum@mi.brandenburg.de
Berlin (BE) Senatsverwaltung für Inneres Lagezentrum Berlin Platz der Lüftbrücke 6 12096 Berlin	Tel.: +49 30 466 490 7210 Fax.: +49 30 466 490 7299 Mail: izberlin@seninn.verwalt-berlin.de
Bréma (HB) Lagezentrum M Polizei Bremen In der Vahr 78 28329 Bremen	Tel.: +49 421 362 1854 or 1754 Fax.: +49 421 362 1859 Mail: Lagezentrum@polizei.bremen.de
Hessen (HE) Hessisches Ministerium des Inneres und für Sport LAGEZENTRUM Friedrich-Ebert-Allee 12 D-65185 Wiebaden	Tel.: +49 611 353 2150 Fax.: +49 611 353 1706 Mail: lzhessen@hmdi.hessen.de

Hamburg (HH) Behörde für Inneres Polizei Hamburg Führungs-und Lagedienst Bruno-Georges-Platz 1 22297 Hamburg	Tel.: +49 40 4286 66055 Fax.: +49 40 4286 66049 Mail: FLDI-FLD2@POLIZEI.HAMBURG.DE
Mecklenburg-Előpomeránia (MV) Innenministerium Mecklenburg-Vorpommern Arsenal am Pfaffenteich Lagezentrum Alexandrinenstrasse 1 19055 Schwerin	Tel.: +49 385 588 2471 (bis -2479) Fax.: +49 385 588 2480 (oder 2481) Mail: lagezentrum@im.mv-regierung.de
Schleswig-Holstein (SH) Landespolizeiamt Gemeinsames Lage- und Führungszentrum Mühlen 166 24116 Kiel	Tel.: +49 431 160 61111 Fax.: +49 431 160 61199 Mail: lob.gifz@polizei.landsh.de
Szászország (SN) Sächsisches Staatsministerium des Innern Landespolizeipräsidium Lagezentrum 01095 Dresden	Tel.: +49 351 564 3775 oder 3776 Fax.: +49 351 564 3779 Mail: Platz2.Lagezentrum@smi.sachsen.de
Szász-Anhalt (ST) Ministerium des Innern des landes Sachsen-Anhalt Lagezentrum Halberstädter Str 2/Am Platz des 17. Juni 39112 Magdeburg	Tel.: +49 391 567 5292 Fax.: +49 391 567 5290 Mail: lagezentrum@mi.lsa-net.de
Thüringia (TH) Thüringer Innenministerium Abteilung 4 -Lagezentrum- Andreasstrasse 38 99084 Erfurt	Tel.: +49 361 37 93 616 Fax.: +49 361 37 93 686 Mail: Lagezentrum@tim.thueringen.de

LUXEMBURG

A luxemburgi jog nem ír elő a szerződés 24. Cikke szerinti közös műveletek beindításához szükséges formális eljárást. Elegendő, hogy kettő vagy több érintett Fél operatív vezetője – Luxemburgban a Nagyhercegségi Rendőrség főigazgatója, vagy az ő képviselője – megegyezzen. A kapcsolatot minden esetben elsőként a Nagyhercegségi Rendőrség Műveleti Osztályával kell felvenni, amelyik a Végrehajtási Megállapodás 14.2 pontja szerinti nemzeti kapcsolattartó pont. Az alábbiak szerint lehet vele kapcsolatba lépni

Police Grand-Ducale
Direction des Opérations
Cím : 1, rue Marie et Pierre Curie
L-2957 LUXEMBOURG
Tel.: + 352 4997 – 2310
Fax : + 352 4997 – 2399
E-mail : dop@police.etat.lu

HOLLANDIA

Országok	Szervezet	Központi kapcsolattartó pont	Telefonszám Faxszám E-mail
AUSZTRIA BELGIUM NÉMETORSZÁG FRANCIAORSZÁG LUXEMBURG SPANYOLORSZÁG	*Korps Landelijke Politie Diensten (KLPD)* Konfliktus- és Válságkezelési Főosztály (*Department for Conflict and Crisismanagement*)	Hoofdstraat 54 Postbus 100 3970 AC Driebergen	Tel: (0031)(0)343 535759 Fax (0031)(0)343 518180 E-mail: ccb-klpd@klpd.politie.nl

---

SPANYOLORSZÁG

A közös műveletekkel kapcsolatos nemzeti jog és hatáskörök

A közös műveletekkel kapcsolatos spanyol jogi szabályozást az alábbi joganyagok tartalmazzák:

- 11/2003-as törvény a közös nyomozócsoportokról. Ez a 2002. június 13-i kerethatározaton alapuló nemzeti jogszabály.
- A határfelügyeletről szóló 40. Cikk szerint ezek a szabályok a schengeni térségben léteznek. Itt a rendes vagy sürgős felügyelet mindig egy igazságügyi nyomozáshoz kötődik, az együttműködési feltételek rögzítik a bűncselekmények típusait, a kompetens spanyol hatóságokat és a felügyelet részleteit, valamint az okmánymintákat.
- Megállapodás Portugáliával a személyek közös és koordinált mobil ellenőrzéséről.

Másféle közös műveletekre, mint a közös őrjáratok, vagy hasonlók, nincs jogi szabályozás.

Spanyolországnak több országgal is van az együttműködés fejlesztését célzó szerződése. Ezek közül kiemelendő:

- **Portugáliával:**
  - Az 1993. február 15-én aláírt visszafogadási megállapodás (mellékelve)
  - Az 1994. január 17-én aláírt megállapodás a mobil ellenőrzésekről (mellékelve)
  - Az 1997. november 19-én aláírt polgári és büntetőügyi megállapodás (mellékelve)
  - Az 1998. november 30-án aláírt megállapodás a forrónyomon való üldözésről (mellékelve)
  - A 2005. november 19-én aláírt megállapodás a határmenti rendőri és vámügyi együttműködésről (mellékelve)

- **Franciaországgal**

  - Az 1998. július 7-én aláírt megállapodás a határmenti rendőri és vámügyi együttműködésről (mellékelve)
  - A 2002. november 26-án aláírt visszafogadási megállapodás (mellékelve)
  - Az Együttműködési Központ szervezeti és működési szabályzata (csak papíralapon áll rendelkezésre)

NEMZETI KAPCSOLATTARTÓ PONT

Spanyolország nemzeti kapcsolattartó pontja:

CENTRO PERMANENTE DE INFORMACIÓN Y COORDINACIÓN (CEPIC)

címe:
Gabinete de Coordinación
Calle Amador de los Rios, 2

28010 MADRID- ESPAÑA

Elérhetőségei: Telefonszámok: + 34 915 371 883
+ 34 915 371 884
+ 34 915 372 056
+ 34 915 372 057
+ 34 915 372 058

FAX: + 34 913 191 228
+ 34 913 191 645
+ 34 913 197 389

E-MAIL: cepic@ses.mir.es

Minta a Szerződés 24. Cikke szerinti közös műveletek iránti megkereséshez

Kérelmező Fél:

❑ A Belga Királyság, amelyet a DGA/DAO nemzeti kapcsolattartó pont igazgatósága képvisel
vagy
❑ A Német Szövetségi Köztársaság, amelyet a .... képvisel
vagy
❑ A Spanyol Királyság, amelyet a .... képvisel
vagy
❑ A Francia Köztársaság, amelyet a .... képvisel
vagy
❑ A Luxemburgi Nagyhercegség, amelyet a Nagyhercegségi Rendőrség főigazgatója, vagy az ő képviselője képvisel
vagy
❑ A Holland Királyság, amelyet a .... képvisel
vagy
❑ Az Osztrák Köztársaság, amelyet a .... képvisel

felkéri

❑ A Belga Királyságot, amelyet a DGA/DAO nemzeti kapcsolattartó pont igazgatósága képvisel
vagy
❑ A Német Szövetségi Köztársaságot, amelyet a .... képvisel
vagy
❑ A Spanyol Királyságot, amelyet a .... képvisel
vagy
❑ A Francia Köztársaságot, amelyet a .... képvisel
vagy
❑ A Luxemburgi Nagyhercegséget, amelyet a Nagyhercegségi Rendőrség főigazgatója, vagy az ő képviselője képvisel
vagy
❑ A Holland Királyságot, amelyet a .... képvisel
vagy
❑ Az Osztrák Köztársaságot, amelyet a .... képvisel

az alábbira:

❑ **Rendőri beavatkozás** …… rendőrtiszttel, a jelen kérelemhez mellékelt részletezés szerint, a közrend fenntartása érdekében az alábbi helyszínen:
…… (*hely, zóna; dátum*);

……...……(*a rendőrtiszt neve és beosztása*) operatív parancsnoksága mellett.
.

❑ **Megállapodásra:**

❑ **Eszközök átadására** a közrend fenntartása érdekében, a jelen kérelemhez mellékelt részletezés szerint

Az eszközöket ……..…… (*a hely neve, a zóna neve; dátum*) fogják használni.

……...(*a rendőrtiszt neve és beosztása*) operatív parancsnoksága mellett.

❑ **Megállapodásra:**

❑ .....……..... rendőrtiszt bevetését az ezt a célt szolgáló anyagi eszközök kíséretére vagy működtetésére.

❑ **Megállapodásra:**

❑ **Egyéb:**

❑ **Megállapodásra:**

❑ **Egy határátlépés**

❑ **Több határátlépés az alábbi időszakban:**

❑ **Megállapodásra:**

Szuverén jogok

❑ Felkéri a szuverén jogkörnek a küldő ország tisztjei számára történő átadására, amit a fogadó ország lehetővé tesz

❑ **Megállapodásra:**

❑ Felkéri, hogy tegye lehetővé a küldő ország tisztjei számára saját szuverén jogaiknak a küldő ország jogrendszere szerinti gyakorlását. Ha ez megtörténik, a küldő állam tisztjeinek ugyanaz lesz a szuverén jogköre, mint saját országukban.

❑ **Megállapodásra:**

Költségek

❑ Minden szerződő Fél a saját hatóságainál felmerült költségeket viseli.

vagy

❑ A költségek megosztására tett egyéb javaslat:

❑ **Megállapodásra:**

……..……..… (*dátum*) ……..……. (*hely*)

…… (*aláírás*)

megállapodás

……..…… (*dátum*) ……..……. (*hely*)

…… (*aláírás*)

D.2 Melléklet

A határon átnyúló műveletben közvetlen veszély esetén haladéktalanul értesítendő hatóságok, és az ebben a Mellékletben felsorolt elérhetőségek változásának bejelentésére szolgáló kapcsolattartó pontok

AUSZTRIA

A szomszédos ország	A szövetségi tartomány vagy minisztérium neve	Települések (a határtelepülések félkövéren vannak szedve)	Telefonszám Faxszám E-mail
Németország	Landespolizeikommando Oberösterreich – Landesleitzentrale		Tel.: +43 (0) 59133 40-2222 Fax: +43 (0) 59133 40-1009 E-mail: LPK-O@polizei.gv.at
	Landespolizeikommando Salzburg – Landesleitzentrale		Tel.: +43 (0) 59133 50-2222 Fax: +43 (0) 59133 50-1009 E-mail: LPK-S@polizei.gv.at
	Landespolizeikommando Tirol – Landesleitzentrale		Tel.: +43 (0) 59133 70-2222 Fax: +43 (0) 59133 70-1009 E-mail: LPK-T@polizei.gv.at
	Landespolizeikommando Vorarlberg – Landesleitzentrale		Tel.: +43 (0) 59133-80-2222 Fax: +43 (0) 59133-80-1009 E-mail: LPK-V@polizei.gv.at
MÁS FELEK	Szövetségi Belügyminisztérium, II. Divízió – Közbiztonsági Főigazgatóság, Műveleti és Válságkoordinációs Központ		Tel.: +431-53126-3200 or -3775 Fax: +431-53126-3120 E-mail: bmi-II-EKC-Permanenzdienst@bmi.gv.at

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

Szövetségi Belügyminisztérium, Közbiztonsági Főigazgatóság,
II/2/a alosztály
Tel.: +431-53126-3411
Fax: +431-53126-10-8638
E-mail: bmi-II-2-a@bmi.gv.at

BELGIUM

NB: Belgiumban a nemzeti központot és az érintett helyi zónát is értesíteni kell!

Nemzeti központ:

DAO
(Direction opérations concernant la police administrative)
Officier de permanence
Blok G, Fritz Toussaintstraat 47
Tél: 02 642 6380
Fax: 02 646 4940
Mail: dga-dao@skynet.be

Helyi rendőrségi zóna

Szomszédos ország	Rendőri zóna száma (és neve)	Települések (a határtelepülések félkövéren vannak szedve)	Telefonszám
FRANCIA-ORSZÁG	PZ 5461 WESTKUST	**DE PANNE** / KOKSIJDE / NIEUWPOORT	+ 32 (0) 58 53.30.00
	PZ 5459 SPOORKIN	**ALVERINGEM** /LO-RENINGE/**VEURNE**	+ 32 (0) 58 33.53.11
	PZ 5462 ARRO IEPER	**HEUVELLAND**/IEPER/LANGE MARK-POELKAPELLE/ MESEN/MOORSLEDE/ **POPERINGE**/ STADEN/VLETEREN/ **WERVIK**/ZONNEBEKE	+ 32 (0) 57 23.05.00
	PZ 5318	**COMINES-WARNETON**	+ 32 (0) 56 55.96.14
	PZ 5455 GRENSLEIE	LEDEGEM /**MENEN**/ **WEVELGEM**	+ 32 (0) 56 51.01.11
	PZ 5317	**MOUSCRON**	+ 32 (0) 56 86.07.00
	PZ 5320 DU VAL DE L'ESCAUT	CELLES/ **ESTAIMPUIS**/ MONT-DE-L'ENCLUS/PECQ	+ 32 (0) 69 53.29.30

Szomszédos ország	Rendőri zóna száma (és neve)	Települések (a határtelepülések félkövéren vannak szedve)	Telefonszám
	PZ 5316 DU TOURNAISIS	**TOURNAI/ANTOING/ RUMES/BRUNEHAUT**	+ 32 (0) 69 25.02.50
	PZ 5321	**BERNISSART/ PERUWELZ**	+ 32 (0) 69 77.20.57
	PZ 5329 DES HAUTS-PAYS	**DOUR/HENSIES/**HONNELLES/ **QUIEVRAIN**	+ 32 (0) 65 65.20.25
	PZ 5327 BORAINE	BOUSSU/COLFONTAINE/ **FRAMERIES**/ QUAREGNON/ SAINT-GHISLAIN	+ 32 (0) 65 61.00.20
	PZ 5324	MONS/QUEVY	+ 32 (0) 65 40.43.00
	PZ 5333 LERMES	**ERQUELINNES / ESTINNES**/LOBBES/MERBES	+ 32 (0) 71 59.76.30
	PZ 5334 BOTTE DU HAINAUT	**BEAUMONT/ CHIMAY**/ FROIDCHAPELLE/ **MOMIGNIES/SIVRY**	+ 32 (0) 60 41.40.70
	PZ 5311 3 VALLEES	**COUVIN /VIROINVAL**	+ 32 (0) 60 31.03.00
	PZ 5315 HERMETON ET HEURE	CERFONTAINE / DOISCHE / PHILIPPEVILLE	+ 32 (0) 71 66.02.11
	PZ 5312 HAUTE-MEUSE	ANHEE / DINANT/ **HASTIERE**/ ONHAYE/YVOIR	+ 32 (0) 82 21.42.98
	PZ 5310 HOUILLE-SEMOIS	**BEAURAING** /BIEVRE/ **GEDINNE/VRESSE-SUR-SEMOIS**	+ 32 (0) 61 58.70.26
	PZ 5302 SEMOIS ET LESSE	BERTRIX/**BOUILLON**/ DAVERDISSE/ HERBEUMONT/ LIBIN/ PALISEUL / SAINT-HUBERT/ TELLIN / WELLIN	+ 32 (0) 61 46.60.07
	PZ 5299 DE GAUME	CHINY /ETALLE/ **FLORENVILLE/ MEIX-DEVANT VIRTON/ ROUVROY**/ TINTIGNY / **VIRTON**	+ 32 (0) 63 58.99.30
	PZ 5298 SUD-LUXEMBOURG	AUBANGE /**MESSANCY**/ **MUSSON**/SAINT-LEGER	+ 32 (0) 63 38.02.54
NÉMET-ORSZÁG	PZ 5292 WESER-GOHL	**EUPEN /KELMIS**/ LONTZEN/**RAEREN**	+ 32 (0) 87 59.55.00
	PZ 5290 STAVELOT-MALMEDY	LIERNEUX / MALMEDY / STAVELOT / STOUMONT / TROIS-PONTS /**WAIMES**	+ 32 (0) 80 28.18.00

Szomszédos ország	Rendőri zóna száma (és neve)	Települések (a határtelepülések félkövéren vannak szedve)	Telefonszám
	PZ 5291 EIFEL	AMEL /**BULLINGEN/ BUTGENBACH/ BURG-REULAND/ SANKT-VITH**	+ 32 (0) 80 28.14.10
LUXEM-BURG	PZ 5298 SUD-LUXEMBOURG	**AUBANGE /MESSANCY/ MUSSON/**SAINT-LEGER	+ 32 (0) 63 38.02.54
	PZ 5297	**ARLON / ATTERT** / HABAY / **MARTELANGE**	+ 32 (0) 63 60.84.49
	PZ 5301 CENTRE ARDENNE	**BASTOGNE** / BERTOGNE / **FAUVILLERS**/LEGLISE/ LBRAMONT-CHEVIGNY/ NEUFCHATEAU/ SAINTE-ODE / VAUX-SUR-SURE	+ 32 (0) 61 24.12.11
	PZ 5300 FAMMENE-ARDENNE	DURBUY / EREZEE / **GOUVY** / HOTTON / **HOUFFALIZE** / LAROCHE-EN-ARDENNE/ MANHAY / MARCHE-EN-FAMENNE/NASSOGNE/ RENDEUX/TENNEVILLE/VIELSALM	+32 (0) 84 31.03.11
	PZ 5291 EIFEL	AMEL /**BULLINGEN/ BUTGENBACH/ BURG-REULAND/ SANKT-VITH**	+ 32 (0) 80 28.14.10
HOLLAN-DIA	PZ 5446	**DAMME / KNOKKE-HEIST**	+ 32 (0) 50 61.96.00
	PZ 5424	**MALDEGEM**	+ 32 (0) 50 72.71.60
	PZ 5417 MEETJESLAND CENTRUM	EEKLO / KAPRIJKE / **SINT-LAUREINS**	+ 32 (0) 9 376.46.46
	PZ 5421	**ASSENEDE** / EVERGEM	+ 32 (0) 9 257.00.10
	PZ 5416 REGIO PUYENBROECK	LOCHRISTI /**MOERBEKE / WACHTEBEKE / ZELZATE**	+ 32 (0) 9 355.74.40
	PZ 5431	**SINT-GILLIS-WAAS/STEKENE**	+ 32 (0) 3 470.27.30
	PZ 5430 BEVEREN	**BEVEREN**	+ 32 (0) 3 750.14.11
	PZ 5345	ANTWERPEN	+ 32 (0) 3 202.55.11
	PZ 5348 NOORD	**KAPELLEN / STABROEK**	+ 32 (0) 3 660.09.30
	PZ 5350 GRENS	**ESSEN** / KALMTHOUT / **WUUSTWEZEL**	+ 32 (0) 3 620.29.29

Szomszédos ország	Rendőri zóna száma (és neve)	Települések (a határtelepülések félkövéren vannak szedve)	Telefonszám
	PZ 5363 NOORDER-KEMPEN	**HOOGSTRATEN / MERKSPLAS /** RIJKEVORSEL	+ 32 (0)3 340.88.00
	PZ 5364 REGIO TURNHOUT	**BAARLE-HERTOG** / BEERSE / KASTERLEE / LILLE / OUD-TURNHOUT / **TURNHOUT** / VORSELAAR	+ 32 (0) 14 40.85.50
	PZ 5367 KEMPEN NOORD-OOST	ARENDONK / **RAVELS** / RETIE	+ 32 (0)14 40.40.60
	PZ 5368	BALEN / DESSEL / MOL	+ 32 (0)14 33.07.00
	PZ 5371	LOMMEL	+ 32 (0)11 54.43.60
	PZ 5372 HANO	**HAMONT-ACHEL** / NEERPELT / OVERPELT	+ 32 (0)11 44.08.20
	PZ 5385 NOORD-OOST LIMBURG	BOCHOLT / BREE / KINROOI / MEEUWEN-GRUITRODE	+ 32 (0)89 48.06.30
	PZ 5383 MAASLAND	DILSEN-STOKKEM / **MAASEIK**	+ 32 (0)89 56.92.11
	PZ 5387	**MAASMECHELEN**	+ 32 (0)89 76 97 00
	PZ 5386	**LANAKEN**	+32 (0)89 71.22.23
	PZ 5381	BILZEN / HOESELT / RIEMST	+ 32 (0)89 51 93 00
	PZ 5281 BASSE-MEUSE	**BASSENGE**/BLEGNY/DALHEM / JUPRELLE / OUPEYE / **VISE**	+ 32 (0)4 374.88.00
	PZ 5382	**VOEREN**	+ 32 (0)4 381.10.11
	PZ 5288 PAYS DE HERVE	AUBEL/BAELEN/HERVE/LIMBOURG/OLNE / PLOMBIERES / THIMISTER-CLERMONT / WELKENRAEDT	+ 32 (0) 87 68.02.40

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

Police Fédérale belge
Direction de la politique en matière de coopération policière internationale (CGI)
Square Victoria Regina 1, 1210 Bruxelles
Tél.: + 32 2 223 98 50
Fax: + 32 2 223 98 82
E-mail: cg.cgi.srt@police.be

FRANCIAORSZÁG

Szomszédos ország	Szervezet	Település	Telefonszám Faxszám E-mail
OLASZORSZÁG	CCPD	Vintimille	Tel: 04 92 41 15 70/71/72 Fax: 04 92 41 15 74 E-mail: ccpd-vintimille.ddpaf-06@interieur.gouv.fr
	CCPD	Modane	Tel: 04 79 05 42 42 Fax: 04 79 05 42 40 E-mail: ccpd-modane-73@wanadoo.fr
NÉMETORSZÁG	CCPD	Kehl	Tel: 0049.7851.8895-0 Fax: 03 90 23 13 69 E-mail: mailto:centro.lz@1.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or: fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)
SVÁJC	CCPD	Genève Cointrin	Tel: 04 50 28 47 00 Fax: 04 50 28 47 19 E-mail: ccpd-geneve.ddpaf-01@interieur.gouv.fr
SPANYOLORSZÁG	CCPD	Hendaye	Tel: 05 59 20 93 60 Fax: 05 59 20 59 34 E-mail: ccpd-hendaye@interieur.gouv.fr
	CCPD	Le Perthus	Tel: 04 68 83 79 00 Fax: 04 68 83 79 10 Tel: 05 59 20 93 60 Fax: 05 59 20 59 34 E-mail: ccpd-hendaye@interieur.gouv.frccpd-sec.le-perthus-66@intermel.si.mi

Szomszédos ország	Szervezet	Település	Telefonszám Faxszám E-mail
	CCPD	Canfranc le Somport	Tel: 05 59 39 04 85 Fax: 05 59 36 18 15 E-mail: ccpd.canfranc@interieur.gouv.fr
	CCPD	Melles Pont du Roy	Tel: 05 61 94 68 40 Fax: 05 61 94 68 48 E-mail: ccpd.melles@interieur.gouv.fr
BELGIUM	CCPD	Tournai	Tel: 00 32 69 68 26 10 Fax: 00 32 69 68 26 21 E-mail: ccpd-tournai.dzaf-59@interieur.gouv.fr
LUXEMBURG	CCPD	Luxembourg	Tel: 03 82 54 94 30 ou +352 26 124 300 Fax: 03 82 54 94 39 ou +352 26 124 199 E-mail: fr@bccp.etat.lu

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

Etat Major de la Direction Centrale de la Police aux Frontières
Centre d'information et de Commandement
Tel: + 33 1 40 07 66 95
Fax: + 33 1 42 65 15 85
E-mail: cic.dcpaf@interieur.gouv.fr

NÉMETORSZÁG

A határt átlépő tiszteknek a tartományi rendőrség kompetens helyi operatív központját vagy a Szövetségi Rendőrséget értesíteniük kell.

Példák határátlépésekre:
„Ad hoc helyzetek” amikor a tisztek öngyilkosságot elkövetni szándékozó vagy segítségre szoruló személyeket találnak; közlekedési balesetek esetén; vagy amikor közvetlen életveszélyt jelentő bűncselekményekre lesznek figyelmesek.

Szomszédos ország	Szervezet	Település	Telefonszám Faxszám E-mail
Az összes prümi partnerrel (AT, FR, LU, BE, NL) meglévő határon	A rendőrség helyi kapcsolattartó pontjai (a tartományi rendőrségek és a Szövetségi Rendőrség) Határátlépés esetén a tartományi rendőrséget és a Szövetségi Rendőrség kompetens helyi rendőrségi kommunikációs központját haladéktalanul tájékoztatni kell	Minden, a prümi partnerekkel meglévő határokon fekvő település	

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

Bundeskriminalamt
65173 Wiesbaden
Tel: +49 611 55 13101
Fax: +49 611 55 12141;
E-mail: mail@bka.bund.de

LUXEMBURG

A határon átnyúló műveletben közvetlen veszély esetén haladéktalanul értesítendő hatóságok

Police Grand-Ducale
Direction des Opérations
Centre d’Intervention National (CIN)
Adresse: 1, rue Marie et Pierre Curie
L-2957 LUXEMBOURG
Tel.: + 352 4997 - 2323

Fax: + 352 4997 – 2398
E-mail: cin@police.etat.lu

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

Police Grand-Ducale
Direction des Opérations et de la Prévention
Adresse: 1, rue Marie et Pierre Curie
L- 2957 LUXEMBOURG
Tel.: + 352 4997 – 2310
Fax: + 352 4997 – 2399
E-mail: dop@police.etat.lu

HOLLANDIA

Szomszédos ország	Szervezet	Elérhetőségei	Telefonszám Faxszám E-mail
BELGIUM NÉMETORSZÁG	Korps Landelijke Politiediensten (KLPD) (Rendőrség) Bureau Conflict-en Crisisbeheersing	Hoofdstraat 54 Postbus 100 3970 AC Driebergen	Tel: (0031)(0)343536366 Fax: (0031)(0)343518180 E-mail: ccb.klpd@klpd.politie.nl

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

Korps Landelijke Politie Diensten (KLPD) Konfliktus- és kríziskezelési Főosztály	Hoofdstraat 54 Postbus 100 3970 AC Driebergen	Tel: (0031)(0)343536366 Fax: (0031)(0)343518180 E-mail: ccb.klpd@klpd.politie.nl

---

SPANYOLORSZÁG

A szerződés értelmében értesítendő hatóságok a alábbiak lesznek:

- A Franciaországgal kötött Schengen-megállapodásban említett operatív egységek.
- A Spanyolország és Franciaország közti Együttműködési Központ, amelynek helye:

Szomszédos ország	Szervezet	Település	Telefonszám Faxszám E-mail Nyitvatartás
FRANCIAORSZÁG	CCPD	LE PERTHUS / LA JUNQUERA	Tel: 00 33 468 837913 Fax: 00 33 468 837920 E-mail: gi-smd-girona-ccpa@guardiacivil.org Nyitvatartás: Hétfő-péntek 08: 00 – 20:30
	CCPD	HENDAYA / IRÚN	Tel: 00 33 559 209360 / 00 34 696 909738 Fax: 00 33 559 205934 E-mail: ss-ccpa-hendaya@guardiacivil.org Nyitvatartás: napi 24 óra
	CCPD	SOMPORT (Huesca)	Tel: 00 34 974 373572 Fax: 00 34 974 373573 E-mail: hu-cmd-huesca-ccpasomport@guardiacivil.org Nyitvatartás: napi 24 óra
	CCPD	MELLES – PONT DU ROY	Tel: 00 33 561 892962 / 00 33 561 946840 Fax: 00 33 561 892639 E-mail: l-ccpa-melles@guardiacivil.org Nyitvatartás: Hétfő–péntek 08: 00 – 21: 00 Szombat–vasárnap 09: 00 – 17: 00

TARTOMÁNYI SZÉKHELY	CÍM	TELEFONSZÁM	FAX	EMAIL INTERNET
GUIPÚZCOA	C/ Barachategui, 59 20015 – San Sebastián	943-276611 (switchboard) 943-297918 Operational Service Center (COS)	943-292134	ss-cmd-sansebastian-cos@guardiacivil.org
NAVARRA	Avda. Galicia, 2 31003 – Pamplona	948-296850	948-296860	na-cmd-pamplona-cos@guardiacivil.org
HUESCA	Avda. Martínez Velasco, 83 22004 – Huesca	974-210074 974-210105 974-210252	974-211238	hu-cmd-huesca-cos@guardiacivil.org
LLEIDA	C/ Libertad, 3 25071 – Lleida	973-249008 (switchboard) 973-245633 (COS)	973-228422 973-246078	l-cmd-lleida-registro@guardiacivil.org
GIRONA	C/ Emilio Grahit, 52 17003 – Girona	972-208650 (switchboard) 972-484012 (COS) 972-426066	972-484000	gi-cmd-girona@guardiacivil.org

NACIONAL POLICE

REGION	UNIT	ADRESS	TELÉFONO	FAX
PAÍS VASCO	Headquarters of San Sebastián	C/ José Mª Salaverria, s/n	34.943.454800	34.943.457855
NAVARRA	Headquarters of Pamplona	C/ General Chinchilla, 3	34.948.299700	34.948.223326
ARAGÓN	Headquarters of Huesca	C/ Ricardo Arco, 7	34.974.245400	34.974.243320
CATALUÑA	Headquarters of Girona	C/ Sant Pau, 2	34.972.220025	34.972.201149
CATALUÑA	Headquarters of Lleida	C/ Paseo de Ronda, 54	34.973.264799	34.973.264799

A jelen Mellékletben feltüntetett elérhetőségek változásának bejelentésére szolgáló nemzeti kapcsolattartó pont:

CENTRO PERMANENTE DE INFORMACIÓN Y COORDINACIÓN (CEPIC)

címe: Gabinete de Coordinación
Calle Amador de los Rios, 2
28010 MADRID – ESPAÑA

Telefonszámok:	FAX:	E-MAIL:
+ 34 915 371 883	+ 34 913 191 228	cepic@ses.mir.es
+ 34 915 371 884	+ 34 913 191 645	
+ 34 915 372 056	+ 34 913 197 389	
+ 34 915 372 057		
+ 34 915 372 058		

D.3 Melléklet

A Szerződés 28. Cikk (1) bekezdés harmadik mondata alapján szállítani tilos fegyverek, lőszerek és felszerelés,

a Szerződés 28. Cikk (2) bekezdés alapján használni tilos fegyverek, lőszerek és felszerelés, illetve a jogi feltételek, a Szerződés 28. Cikk (5) bekezdés szerinti gyakorlati feltételek

AUSZTRIA

Ausztriában nincs a szerződés 28. Cikk (1) bekezdés harmadik mondata és a 28. Cikk (2) bekezdés harmadik mondata szerinti tilalom.

A FEGYVEREK, LŐSZEREK ÉS FELSZERELÉS HASZNÁLATÁNAK JOGI ÉS GYAKORLATI FELTÉTELEI

A Szövetségi Jogi Közlöny 149/1969 számában kihirdetett 1969. március 27-i, a „Szövetségi Rendőrség, a Szövetségi Csendőrség és a települési rendőrség tisztjeinek fegyverhasználatáról” szóló szövetségi törvény (1969-es fegyverhasználati törvény) szabályozza a kényszerítő eszközök és szolgálati fegyverek használatát.

2. § A Szövetségi Rendőrség, a Szövetségi Csendőrség és a települési rendőrség tisztjei munkájuk végzése során, amennyiben szükséges, használhatják szolgálati fegyvereiket

1. jogos védelem esetén;
2. a jogszerű rendészeti beavatkozásnak való ellenállás leküzdésére;
3. jogszerű letartóztatás foganatosításra;
4. egy fogvatartott személy szökésének magakadályozására;
5. a veszély bármely formájának elhárítására.

3. § A szövetségi törvény értelmezésében szolgálati fegyvernek minősülnek:

1. a gumibotok, és a rendőri beavatkozásra alkalmas más botok,
2. a könnygáz és más irritatív szerek, amelyek csak rövid ideig tartó egészségkárosodást okoznak,
3. a vízágyúk,
4. a Szövetségi Jogi Közlöny 152/1955-ös számában kihirdetett, a „független és demokratikus Ausztria visszaállításáról” szóló szövetségi törvény I. Mellékletének 1. és 2. bekezdésében az I. kategóriába sorolt lőfegyverek, amelyek a 2. §-ban felsorolt tiszteket az elöljárójuk utasítására végzett munkájukban segítik.

4. § A fegyverek használata csak akkor megengedett, ha az enyhébb intézkedések, mint pl. a jogszerű állapot visszaállítására adott parancs, a lőfegyverek használatával való fenyegetés, egy szökevény üldözése, testi erő alkalmazása, vagy más rendelkezésre álló enyhébb eszköz, mint a bilincs vagy a műszaki akadályok nem bizonyultak megfelelőnek vagy elég hatékonynak

5. § Ha különböző típusú fegyverek állnak rendelkezésre, csak a legkevésbé veszélyesnek tűnő, de a fennálló körülmények közt még hatásos fegyver használható.

6. § (1) Fegyvereket emberek ellen használni csak az ellenállásra vagy a szökésre képtelenné tételük érdekében lehet. A 2. § 2–5. bekezdésében leírt esetekben a fegyverek használata által okozott kárnak arányosnak kell lennie az elérni kívánt hatással.

(2) Minden fegyvert a lehető legnagyobb óvatossággal, és az emberekre és tárgyakra való tekintettel kell használni. A fegyvereket csak akkor lehet emberek ellen bevetni, ha tárgyak ellen nem lenne hatékony.

Fegyverek életveszélyt okozó használata

7. § Az emberek életét veszélyeztető fegyverek használata csak az alábbi esetekben megengedhető:

1. jogos védelemre egy ember megvédésére;
2. zavargás vagy felkelés letörésére;
3. egy csak szándékosan elkövethető, és több mint egy éves börtönbüntetéssel fenyegetett bűncselekménnyel alaposan gyanúsítható személy letartóztatásának foganatosítására, vagy szökésének magakadályozására, amely önmagában, vagy a gyanúsítottnak a letartóztatás vagy a menekülés során tanúsított magatartása kapcsán azt mutatja, hogy az államra, az elkövetőre vagy tárgyakra általános biztonsági kockázat áll fenn,
4. egy saját magára, vagy tárgyakra általános biztonsági kockázatot jelentő, szellemileg zavart személy szökésének megakadályozására.

8. § (1) Egy megkülönböztető figyelmeztető jelzést kell adni közvetlenül a fegyverek emberek elleni életet veszélyeztető használata előtt. Tömeg esetén a figyelmeztetést meg kell ismételni. Figyelmezető lövés leadása is figyelmeztetésnek számít.
(2) A fegyverek életet veszélyeztető használata csak akkor megengedett, ha az az ártatlan emberek számára nem jelent kockázatot, kivéve, ha ez elkerülhetetlennek tűnik egy tömeg által elkövetendő, személyeknek közvetlenül vagy közvetetten biztonsági kockázatot jelentő erőszakos cselekmény megakadályozásához.
(3) Jogos védelem esetén az 1. és a 2. bekezdés rendelkezései nem alkalmazandóak.

Szolgálati fegyvereken, illetve fegyverhatású eszközökön kívüli eszközök használata

9. § Ha nem áll rendelkezésre megfelelő szolgálati fegyver, más fegyvereket, illetve fegyverhatású eszközöket is lehet alkalmazni, a szövetségi törvény rendelkezéseinek *mutatis mutandis* alkalmazásával.

BELGIUM

Szállítani tilos fegyverek, lőszerek és felszerelés

A 25. Cikk szerinti határon átnyúló együttműködésre: Belgiumban nincs tilalom. A határon átnyúló együttműködés más formáira: a rendőrtisztek azon fegyvereket, lőszereket és felszerelést szállíthatják, amelyeket Belgiumban is használhatnak.

Használni tilos fegyverek, lőszerek és felszerelés

Belgium a szerződés 2. Mellékletében felsorolt fegyverek, lőszerek és felszerelés használatát engedélyezi. A küldő ország Belgium területén tevékenykedő tisztjének az alábbi alapelveket kell követnie:

- Belgium nem engedélyezi a 9 mm-nél nagyobb kaliberű lőfegyverek használatát;
- Belgium nem engedélyezi a lőfegyverek teljesen automatikus módban történő használatát;
- Belgium nem engedélyezi az olyan bilincsek használatát, amelyek a letartóztatott személyeknek sérülést okozhatnak;
- Belgium engedélyezi a paprikaspray használatát, de nem engedélyezi a kloro-acetofenon (CN) könnygáz használatát;
- Belgium nem engedélyezi az elektromos botok használatát, de engedélyezi a hagyományos botokét;
- Belgium nem engedélyezi a TASER (elektromos sokkoló) használatát.

Az engedélyezett fegyverek, lőszerek és felszerelés jogi és gyakorlati feltételei (28. Cikk)

1. Önvédelem

Rendőrségi törvény 38. Cikke

A 37. cikk sérelme nélkül, a rendőrök csak önvédelem során használhatnak emberek ellen lőfegyvert.

Büntető törvénykönyv 416. Cikke

A jogos önvédelem során elkövetett emberölés vagy testi sértés nem tekinthető bűntettnek vagy vétségnek.

Büntető törvénykönyv 416. Cikkének magyarázata

- Az önvédelem mindenkire, nem csak a rendőrökre alkalmazandó
- Az önvédelem az erőszak minden fajtája ellen irányulhat, nem csak a lőfegyverek ellen.
- Ahhoz, hogy önvédelemnek lehessen tekinteni, a szituáció meg kell, hogy feleljen az alábbi követelményeknek:

  * **A támadás megkezdődött, vagy épp most kezdődik.**
    Az áldozatnak nem feltétlenül kell életveszélyben lennie. Elég, ha valódi és jelentős kockázata áll fenn sérülésének.
    A támadás jogszerűtlen.
    Jogszerű és indokolt támadás ellen nincs hely önvédelemnek. Így például nem megengedett a jogszerű rendőri intézkedések ellen az erőszak alkalmazása.
  * **A támadásnak emberek ellen kell irányulnia.**
    A büntető törvénykönyv 416. Cikke szerint a szóbeli sértés vagy fenyegetés nem tekinthetők emberek elleni támadásnak.
  * **Az önvédelemnek szükségesnek és arányosnak kell lennie.**
    Ha az önvédelem túlmegy a szükséges határokon, ha a védekezés erőszakosabb a támadásnál, akkor szintén támadássá válik. Ami az arányosságot illeti, a fegyverhasználat következményeit mindig figyelembe kell venni. Fejbeverni valakit ugyanolyan halálos lehet, mint egy lövés. Ha valaki nem tudja magát máshogy megvédeni, és életveszélyben van, akkor a lőfegyver használata indokolt.
  * **A védekezésnek a támadással egyidejűleg kell történnie.**
    Az önvédelem nem lehet bosszú, és ebből adódóan nem történhet a támadás befejezése után.

Büntető törvénykönyv 417. Cikke
A büntető törvénykönyv 416. Cikkének rendelkezései mellett két másik esetet lehet még önvédelemnek tekinteni. Ezeket a büntető törvénykönyv 417. Cikke magyarázza meg.

Mindkét alábbi esetet jogos védelemnek lehet tekinteni:

1. Ha az emberölést vagy testi sértést annak során követték el, hogy éjszaka valaki egy kerítésen vagy falon átmászva betört egy házba, lakásba, vagy melléképületbe, kivéve, ha a rendőr feltételezése szerint nem állt szándékában az emberölési kísérlet az általa elkövetett cselekmény előtt, vagy a lakók ellenállásának következményeként.
2. Ha az esemény lopás vagy rablás elkövetői elleni védekezés során testi sértéssel és bántalmazással történt.

Figyelmeztetés adása.

A rendőrségi törvény 37. Cikkével összhangban erő bármilyen alkalmazását meg kell előznie egy figyelmeztetésnek, kivéve, ha a figyelmeztetés ennek hatékonyságát rontaná. A lényeges itt az, hogy a lőfegyvert preventív módon és megtorlásra is lehet használni. A lőfegyver preventív jellegű használatába beleértendő az ellenfél megfélemlítése. Ebben az esetben nem történik lövés, a lőfegyvert csak preventív módon használták.

A megtorlás jellegű használat három fajtáját lehet megkülönböztetni:

a. Megfélemlítési lövés. A megfélemlítési lövést akkor kell leadni, ha a rendőrt nem fenyegeti közvetlen veszély. A levegőbe tüzel, hogy megfélemlítse ellenfelét.
b. Figyelmeztető lövés. A figyelmeztető lövést akkor kell leadni, amikor a rendőrt veszély fenyegeti. Ebben az esetben nem tüzel az ellenfélre.
c. Emberekre, állatokra vagy tárgyakra leadott lövés. Ez történhet önvédelem esetén, vagy a rendőrségi törvényben meghatározott esetekben.

Röviden, megállapíthatjuk, hogy az erő alkalmazását egy figyelmeztetés előzi meg. A figyelmeztetés lehet egy szóbeli felszólítás, vagy egy figyelmeztető lövés, amennyiben ez a figyelmeztetés nem rontja az erő alkalmazásának hatékonyságát, vagy önvédelem esetén.

2. Erő alkalmazása

Belgiumban a lőfegyvereket és a lőszereket csak jogos védelem esetén lehet használni. A Szerződés 28. Cikk (2) bekezdése alapján azonban a műveletért felelős belga rendőrtiszt egyedi esetben, az önvédelmen kívüli célból is engedélyezheti más engedélyezett fegyverek használatát. Ezen fegyverek és felszerelés használatának azonban minden esetben összhangban kell állnia a belga nemzeti joggal.

Rendőrségi törvény 37. Cikke

Feladatai végrehajtása során minden rendőrtiszt alkalmazhat erőt, az alábbi feltételekkel:

1. Az erő alkalmazásának minden kockázatát figyelembe kell vennie;
2. Jogszerű célra kell irányulnia (amit máshogyan nem lehet elérni);
3. Az erő alkalmazása megfelelő és arányos kell, hogy legyen az elérendő cél tekintetében;
4. Az erő alkalmazását meg kell, hogy előzze egy figyelmeztetés (kivéve, ha ez rontaná annak hatékonyságát).

A 37. Cikk magyarázata

A 37. Cikk első három feltételét egy-egy szóba lehet sűríteni:

1. Lehetőség: a rendőrnek figyelembe kell vennie az erő alkalmazásának kockázatait, testi és anyagi szempontból is. Pl.: egy ellenőrzés során a rendőr egy távozó jármű kerekére lő, de a golyó célt téveszt, és egy ártatlan járókelőt talál el.
2. Jogszerűség: az erő és a kényszer alkalmazása csak a jogszabályok által megengedett esetekben és feltételekkel történhet Pl.: egy személyazonosság-ellenőrzés során az ellenőrzött személy meg akarja ütni a rendőrt, erre egy másik rendőrnek azonnal reagálni kell, önvédelemmel.

3. Arányosság: ha az erő és kényszer alkalmazása szükséges, a kevésbé erőszakos és legmegfelelőbb megoldást kell választani. Pl.: egy kocsmai verekedésben egy ittas személy megragad egy üveget, és úgy tesz, mintha megütne vele egy másik személyt. Az ittas személy nem reagál a szóbeli figyelmeztetésre. Mivel ez a személy ittas és felfegyverkezett, gumibottal lehet megkísérelni a leküzdését.

Röviden, az erő alkalmazása előtt három kérdést kell feltenni magunknak:

1. Jogszerű-e?
2. Nincs-e más, kevésbé erőszakos és veszélyes eszköz?
3. Arányosak-e az eszközök az elérendő céllal?

FRANCIAORSZÁG

Franciaország nem ír elő semmilyen korlátozást a szolgálati fegyverek, kényszerítő eszközök, vagy más felszerelés szállítására, amennyiben ezeket a prümi partnerek rendőri szervei adták ki.

A 25. cikk alkalmazása során a fegyverek használatát az önvédelmi helyzetekre kell korlátozni, és csak a kézifegyverek (revolverek és pisztolyok), könnygáz és gumibotok megengedettek, amennyiben ezeket a rendőri szervek adták ki

A fegyverek, lőszerek és felszerelés jogi és gyakorlati feltételei

A jogos védelem speciális feltételei

A francia büntetőjogban az önvédelmet a büntető törvénykönyv 122-5 és 122-6 cikkei írják le. Míg előbbi az önvédelem általános feltételeit, a második két konkrét esetet ír le, amelyekre adott reakció önvédelemnek lesz tekintendő.

Elsőként, az önvédelem egy reakció egy áldozatnak egy támadástól való megvédésére, a 122-5 cikk pedig ennek két összetevőjét, a támadást és az ellentámadást határozza meg.

A támadást egy személy ellen követik el, akár rendőr, akár nem. Jogszerűtlennek kell lennie, ami nyilvánvalóan nem áll fenn a rendőri intézkedéseknek való ellenállás esetében. Végül valósnak és jelenidejűnek kell lennie, ami egyrészt azt jelent, hogy a fegyverek használatát egy fenyegetésre adott reakcióként nem lehet önvédelemként igazolni, másrészt hogy a fegyvernek a támadás befejezése utáni használata bosszúnak, nem pedig önvédelemnek tekintendő.

Az imént említett okokból az ellentámadásnak azonnal kell követnie a támadást, hogy ne bosszúnak minősüljön. Szükségesnek is kell lennie, ami azt jelenti, hogy csak ezzel állítható meg a támadás. Végül, arányosnak kell lennie a támadással.

Másodszor, az önvédelem egy bűncselekmény vagy tulajdon elleni támadás megszakítását célzó egyidejű reakció. Ebben a helyzetben a 122-5 cikk szerint az önvédelemnek szükségesnek és az elkövetett tett súlyával arányosnak kell lennie, amennyiben az nem emberölés.

A 122-5 cikk szerint az önvédelemből cselekvő személynek nincs büntetőjogi felelőssége.

A 122-6 cikk két konkrét helyzetről szól, amelyekben a fegyver rendőr általi használata önvédelmi célúnak tekintendő. Az első az az eset, amikor a rendőr egy lakott ingatlanból távolítja el egy erőszakkal vagy megtévesztéssel elkövetett betörés tettesét. A második az, amikor a rendőr magát egy erőszakkal elkövetett lopás vagy rablás elkövetőivel szemben védi meg. A 122-6 cikkben írtak nem kérdőjelezhetőek meg, és nem mentesítik az önvédelemből cselekvő személyt a 122-5 cikkben rögzítettek alól, mint pl. a súlyos, valós és közvetlen veszély megléte.

A büntető eljárási törvény 73. cikkében leírt konkrét helyzet

Ez a Cikk azt mondja ki, hogy egy bűncselekményt észlelő állampolgár feltartóztathatja annak elkövetőjét, hogy átadja a helyi rendőrtisztnek. Tehát a Szerződés 25. Cikkének alkalmazásában a francia határt átlépő külföldi rendőrtiszt őrizetbe vehet egy bűnelkövetőt, feltéve, hogy tettenéri.

NÉMETORSZÁG

A határokon átnyúló műveletekben szállítani tilos fegyverek, lőszerek és felszerelés (28. Cikk)

Mindenfajta műveletre: nincs tilalom

Engedélyezett fegyverek, lőszerek és felszerelés használatának jogi és gyakorlati feltételei:

Németországban a rendőrtisztek általi közhatalmi erőszak alkalmazásánál a közvetlen kényszer alkalmazásáról szóló törvény ("*Gesetz über den unmittelbaren Zwang bei Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Bundes (BGBl. I 1961, 165)"*); legutóbb a 2006. október 31-i Art. 28 V módosította) és a szövetségi tartományok ennek megfelelő jogszabályai az irányadóak.

LUXEMBURG

Szállítani tilos fegyverek, lőszerek és felszerelés

A Szerződés 24. és 25. Cikke szerinti, határokon átnyúló közös műveletekre alapestben nincs tilalom, a többi Fél rendőrtisztjei szállíthatnak szokásos egyéni vagy csapatfelszerelésük részét képező fegyvereket, lőszereket és felszerelést.

A Szerződés 24. Cikke szerinti közös műveletekre a Végrehajtási Megállapodás 14.1 pontjában előírt feladat-meghatározás rögzítheti az egy adott műveletben nem szállítható felszereléseket.

Használni tilos fegyverek, lőszerek és felszerelés

Luxemburg megengedi a Szerződés 2. Mellékletében felsorolt fegyverek, lőszerek és felszerelés használatát. A küldő ország luxemburgi területen tevékenykedő tisztjeinek az alábbi elveket kell figyelembe venniük:

Engedélyezett fegyverek, lőszerek és felszerelés használatának jogi és gyakorlati feltételei

1. Önvédelem:

A luxemburgi rendőröket – és így a többi Félnek a Szerződés értelmében luxemburgi területen tevékenykedő rendőreit is – az önvédelemnek a büntető törvénykönyv 416. és 417. cikke szerinti általános szabályai kötik, amely szerint a jogos védelem során elkövetett emberölés vagy testi sértés nem tekinthető bűntettnek vagy vétségnek. Az önvédelmet nem csak lőfegyverek ellen, hanem minden testi erőszak ellen is lehet alkalmazni.

Az önvédelemként való elfogadhatósághoz az alábbi feltételeknek kell teljesülniük:

1) *A támadásnak jogszerűtlennek kell lennie.*
   A jogszerű és indokolt támadás ellen nincs helye önvédelemnek. Például jogszerű rendőri fellépés ellen nem szabad erőszakot alkalmazni.
2) *Az önvédelemnek a támadással egyidejűleg kell történnie.*
   Az önvédelemnek legkésőbb akkor kell megkezdődnie, amikor a támadás még folyamatban van; a támadás befejezését követő bármilyen védekezés nem tekinthető önvédelemnek. Ezért egy menekülő elleni testi erőszak, vagy a bosszú kívül esik az önvédelem körén.
3) *Az önvédelemnek szükségesnek és arányosnak kell lennie.*
   Egy támadás elkerüléséhez szükséges határokon túlmenő, halál vagy testi sérülés kockázatát jelentő cselekmény támadássá válhat. Egy fegyver használatának következményeit mindig figyelembe kell venni. Fejbeverni valakit például ugyanolyan halálos lehet, mint egy lövés. Ha valaki nem tudja magát máshogy megvédeni, és életveszélyben van, akkor a lőfegyver használata indokolt. Ami az arányosságot illeti, hangsúlyozni kell, hogy egy, a támadásnál erőszakosabb védekezés támadássá válhat. Másfelől, az áldozatnak nem feltétlenül kell életveszélyben lennie; sérülésének valós és súlyos kockázata is elegendő ehhez.
4) *A támadásnak testi erőszakból kell állnia.*
   A sértések vagy szóbeli támadások nem tekinthetőek önvédelmet igazoló támadásnak.

5) *Az önvédelmet alapesetben emberek elleni támadás során lehet alkalmazni.*
Egy harmadik személy támadás elleni védelme is önvédelemnek tekintendő, ha az összes többi feltétel teljesül. Ezen túlmenően, a tárgyakkal kapcsolatos önvédelem is elfogadható elvileg, de az arányosság követelményét ebben az esetben nehéz teljesíteni. Egy lopáson ért személy megsebesítése vagy halála alapvetően soha nem tekinthető önvédelemnek.

Az önvédelmi helyzet mellett két olyan eset van, ami jogos védelemnek tekinthető:

b) Ha az emberölést vagy testi sértést annak során követték el, hogy éjszaka valaki egy kerítésen vagy falon átmászva betört egy házba, lakásba, vagy melléképületbe, kivéve, ha a rendőr feltételezése szerint nem állt szándékában az emberölési kísérlet az általa elkövetett cselekmény előtt, vagy a lakók ellenállásának következményeként.
c) Ha az esemény lopás vagy rablás elkövetői elleni védekezés során testi sértéssel és bántalmazással történt.

2. A rendőri erő használata, eltekintve az önvédelmi esetektől:

Az önvédelemre vonatkozó szabályok mellett a rendőrök Luxemburgban a fegyvereknek és más kényszerítő eszközöknek a karhatalmi erők által a bűncselekmények elleni küzdelemben való használatáról szóló 1973. július 28-i törvény alapján használhatnak fegyvereket, lőfegyvereket és egyéb kényszerítő eszközöket.

E törvény rendelkezései az alábbiakban összegezhetők:
A szolgálatban lévő rendőrtisztek, ha ez feltétlenül szükséges, akkor használhatnak fegyvereket vagy más eszközöket:
1) Ha fegyverrel, vagy fegyvertelenül megtámadják őket;
2) Ha olyan személynek segítenek ezzel, akinek az élete, testi épsége vagy tárgyai jelentősen veszélyeztetettek;
3) Ha ez az egyetlen mód személyek, helyszínek, épületek, vagy más megvédendő tárgyak fegyveres vagy fegyvertelen megtámadása ellen;
4) Ha a két alkalommal „Állj, rendőrség!” felkiáltással felszólított személyek nem állnak meg, máshogy nem állíthatóak meg, utóbbi esetben azonban a fegyverek használata csak akkor indokolt, ha okkal feltételezhető, hogy:
   a) ezek az azonosított vagy azonosítatlan személyek egy bűncselekményt követtek el;
   b) ezeket a személyeket bűncselekmény miatti elfogatóparancs alapján körözik;
   c) ezek a személyek szökött rabok, vagy elítélt személyek.

A rendőrök az alábbi feltételek teljesülése esetén is használhatják fegyvereiket:
1) egy támadást követően menekülő személyek ellen, és azok ellen, akik a felszólítást követően nem álltak meg;
2) rabokat, elkobzott vagy lefoglalt tárgyakat vagy bizonyítékokat hatalmába kerítését megkísérlő személy ellen;
3) ha egy jármű, hajó, vagy légijármű megállítására nincs más mód;
4) egy bűncselekmény vagy vétség közvetlen elkövetésének megakadályozására.

A fent említett fegyverhasználat a pénz és más értékek szállításának védelmére is megengedett.

Az 1973. július 28-i, fent említett törvény részletes rendelkezéseit az alábbiakban francia és német nyelven közöljük, kivonatosan.

Loi du 28 juillet 1973 réglant l´usage des armes et autres moyens de contrainte par les membres de la force publique dans la lutte contre la criminalité.
(Extrait)

Art. 1er. Dans l'exercice de leurs fonctions, les membres de la police grand-ducale peuvent, en cas de nécessité absolue, faire usage des armes blanches ou des armes à feu dans les cas suivants:

5) lorsque des violences ou voies de fait sont exercées contre eux, ou lorsqu'ils sont attaqués même sans armes ou qu'ils sont menacés par des individus armés;
6) lorsqu'ils sont appelés à prêter assistance à des personnes attaquées et dont la vie, l'intégrité physique ou les biens sont exposés à un danger considérable et présent;
7) lorsqu'ils ne peuvent défendre autrement, contre une attaque armée ou non, le terrain qu'ils occupent, les postes, édifices et installations qui leur sont confiés ou qui sont sous leur garde, ou encore les personnes à eux confiées ou sous leur escorte;
8) lorsque les personnes sommées de s'arrêter par deux appels, faits à haute voix, de «Halte, police !», cherchent à se soustraire à leurs investigations ou à l'arrestation, et ne peuvent être contraintes de s'arrêter que par l´usage des armes; toutefois, dans ce cas l'usage des armes n'est justifié que s'il y a des présomptions graves:
   a) que les individus en question, identifiés ou non, ont commis un crime, et notamment s'ils sont poursuivis par la clameur publique;
   b) ou que ces individus sont des personnes recherchées ou dont l'arrestation est ordonnée par un mandat de justice, pour crime;
   c) ou que ces individus sont des prisonniers, détenus ou condamnés évadés, et qui sont recherchés, inculpés ou condamnés du chef de crime.

Art. 2. Les membres de la police grand-ducale peuvent encore faire usage de leurs armes, dans les conditions spécifiées à l'article 1er:

1) contre les personnes qui, sans obéir à l'ordre de s´arrêter, fuient après les avoir attaqués à main armée, et contre les conducteurs de véhicules pourvus de moteurs mécaniques qui fuient après avoir manœuvré pour mettre leur vie en péril;
2) pour repousser ceux qui, malgré la sommation de se désister ou de s'éloigner, tentent de leur enlever leurs prisonniers, leurs armes ou les objets saisis en vue de la confiscation ou à titre de pièces de conviction;
3) lorsqu'ils ne peuvent immobilier autrement les véhicules, embarcations, aéronefs ou autres moyens servant au transport d´auteurs présumés d´un crime dont les conducteurs n'obtempèrent pas à l'ordre ou au signal d'arrêt, sans préjudice de ce qui est porté à l'article 8 ci-après; lorsqu'un barrage dressé dans le cadre de la recherche des malfaiteurs a été forcé par un véhicule, et s'il appert des circonstances qu'il l'a été en connaissance de cause, le feu peut être ouvert sans sommation;
4) pour empêcher la commission imminente d'une infraction ou la continuation de cette infraction, si, d´après les circonstances, celle-ci constitue soit un crime, soit un délit commis à l'aide d´armes ou d´explosifs.

Art. 3. Dans les cas où il y a rébellion de la part des prisonniers ou tentative d'évasion, et s'il n'y a pas d'autres moyens de contenir ou de contraindre les révoltés ou les fuyards, le chef de l'escorte leur enjoint de rentrer dans l´ordre par les mots: «Halte ou je fais feu». Si cette injonction n'est pas suivie, l'usage des armes est autorisé.
Si les prisonniers cherchent à s'emparer des armes des membres de l'escorte, ou fuient après avoir blessé un membre de celle-ci, les armes peuvent être employées à l'instant et sans sommation préalable.

Art. 4. (…)

Art. 5. (…)

Art. 6. En cas de transport de fonds ou valeurs publics ou privés, les membres de la force publique qui forment l'escorte, en exécution des ordres reçus, peuvent ouvrir le feu dès qu'une attaque contre le convoi se manifeste par des actes extérieurs qui en forment un commencement d´exécution même s'ils ne sont pas personnellement en état de légitime défense. Si les assaillants fuient après s'être emparés de tout ou partie des valeurs convoyées, le feu peut être ouvert sur eux et leurs véhicules sans sommation.

Art. 7. Les prescriptions des articles 1 à 4 et 6 s'appliquent également à l'usage des gaz lacrymogènes et du matériel d´arrosage.

Art. 8. Dans le cadre de leurs opérations de contrôle et de recherche, les fonctionnaires visés à l'article 1er opérant d'office ou sur les ordres de leurs supérieurs hiérarchiques ou sur la réquisition de l'autorité judiciaire peuvent immobilier les véhicules de toute nature au moyen de câbles, herses, hérissons, barrières, filets et autres engins analogues.

Art. 9. (…)

Art. 10. Lorsque, dans l´exercice de ses fonctions, un membre de la force publique a reçu de son supérieur l'ordre d'employer les armes ou un moyen de contrainte quelconque, cet ordre est à exécuter, à moins qu'il ne concerne pas l'exécution des fonctions.
L'ordre ne doit pas être exécuté, si son exécution constituait un crime ou un délit.
Si, dans ce cas, l'ordre est néanmoins exécuté, l'agent d'exécution n'est responsable que s'il a connu ou pu connaître d'après les circonstances qu'il s'agissait manifestement d'un crime ou délit.
L'agent d'exécution doit, si les circonstances le lui permettent, faire valoir à l'égard de l'auteur de l'ordre ses objections en ce qui concerne la légalité de l'ordre reçu.

Art. 11. La présente loi ne déroge ni aux dispositions légales concernant le droit de légitime défense, ni aux dispositions de lois particulières qui autorisent, dans certains cas et au profit de certains agents et fonctionnaires, l'emploi de moyens de contrainte ou l'usage des armes dans une mesure plus étendue.
(…)

Gesetz vom 28. Juli 1973 über die Reglementierung des Gebrauchs von Waffen und anderen Zwangsmittel durch die Mitglieder der öffentlichen Macht im Kampfe gegen die Kriminalität. (Auszug)

Art. 1. Die Mitglieder der grossherzoglichen Polizei können, in Ausübung ihrer Pflicht und im Falle absoluter Notwendigkeit, in folgenden Fällen Gebrauch von Blank- oder Schusswaffen machen:

1) wenn Gewalttätigkeiten oder Tätlichkeiten gegen sie ausgeübt werden, oder wenn sie angegriffen werden, selbst ohne Waffen, oder wenn sie von bewaffneten Individuen bedroht werden;
2) wenn sie angegriffenen Personen Beistand leisten sollen, deren Leben, physische Unversehrtheit oder Eigentum einer beträchtlichen und gegenwärtigen Gefahr ausgesetzt sind;
3) wenn sie das von ihnen besetzte Gelände, die ihnen anvertrauten oder unter ihrer Bewachung stehenden Posten, Gebäude und Einrichtungen, oder aber die ihnen anvertrauten oder von ihnen eskortierten Personen nicht anders gegen einen bewaffneten oder nicht bewaffneten Angriff verteidigen können;
4) wenn die durch zwei, mit lauter Stimme gemachten Aufforderungen « Halt, Polizei ! » zum Stehen bleiben aufgeforderten Personen versuchen, sich ihrer Untersuchung oder Verhaftung zu entziehen, und nicht anders als durch den Gebrauch von Waffen zum Stehen bleiben gezwungen werden können; jedoch ist der Waffengebrauch in diesem Falle nur gerechtfertigt, wenn ernsthafte Vermutungen vorhanden sind:
   a) dass die betreffenden Individuen, ob identifiziert oder nicht, ein Verbrechen begangen haben, und besonders wenn sie vom öffentlichen Nachruf verfolgt werden;
   b) oder dass diese Individuen wegen eines Verbrechens gesucht werden, oder ihre Verhaftung wegen eines Verbrechens gerichtlich angeordnet worden ist;
   c) oder dass es sich bei diesen Individuen um entflohene Gefangene, Inhaftierte oder Verurteilte handelt, die wegen eines Verbrechens gesucht, beschuldigt oder verurteilt sind.

Art. 2. Die Mitglieder der grossherzoglichen der Polizei können, gemäss den in Artikel 1 bezeichneten Bedingungen, auch ihre Waffen gebrauchen:

1) Gegen Personen welche dem Befehl Stehen zu keine Folge leisten, die Flucht ergreifen nachdem sie die Beamten mit bewaffneter Hand angegriffen haben, sowie gegen die Fahrer von Kraftfahrzeugen die flüchtig werden, nachdem sie manövriert haben um das Leben der Beamten in Gefahr zu bringen;
2) Um diejenigen abzuwehren die, trotz Aufforderung von ihrem Vorhaben zu lassen oder sich zu entfernen, versuchen ihnen ihre Gefangenen, ihre Waffen oder die zwecks Einziehung oder als Beweisstücke beschlagnahmten Gegenstände zu entreissen;
3) Wenn sie nicht anders Fahrzeuge, Boote, Luftfahrzeuge oder sonstige Mittel zum Stillstand bringen können, die zur Beförderung der mutmaßlichen Urheber eines Verbrechens diesen und deren Fahrer dem Befehl oder dem Signal zum Halten keine Folge leisten, dies unbeschadet der Bestimmungen des nachstehend angeführten Artikels 8; das Feuer kann ohne Aufforderung eröffnet werden, wenn eine im Rahmen einer Fahndung errichtete Verkehrssperre von einem Kraftfahrzeug durchbrochen wurde, und sich aus dem Umständen ergibt, dass dies in voller Kenntnis der Sachlage geschehen ist;

4) Um das unmittelbar bevorstehende Begehen einer Zuwiderhandlung, oder um die Fortsetzung dieser Zuwiderhandlung zu verhindern wenn, den Umständen gemäss, es sich dabei um ein Verbrechen oder um ein mittels Waffen oder Sprengstoffen begangenes Vergehen handelt.

Art. 3. Wenn im Falle einer Rebellion oder eines Fluchtversuches von Gefangenen es nicht anders möglich ist die Rebellierenden oder Flüchtenden zurückzuhalten oder zu bezwingen, so befiehlt ihnen der befehlshabende Beamte die Ordnung wiederherzustellen mit den Worten « Halt oder ich schieße ! ». Wird diesem Befehl keine Folge geleistet, so ist der Gebrauch von Waffen erlaubt.

Die Waffen können sofort und ohne vorherige Aufforderung gebraucht werden wenn die Gefangenen versuchen sich der Waffen der Beamten zu bemächtigen oder flüchtig werden, nachdem sie einen dieser Beamten verwundet haben.

Art. 4. (…)

Art. 5. (…)

Art. 6. Sobald im Falle eines Geldtransportes oder eines Transportes von öffentlichen oder privaten Werten sich ein Angriff auf den Transport durch äußere Handlungen bemerkbar macht, die einen Anfang der Ausführung bilden, können die in Ausführung der erhaltenen Befehle die Eskorte bildenden Beamten das Feuer eröffnen, selbst wenn sie sich persönlich nicht im Zustand der rechtmäßigen Verteidigung befinden. Gehen die Angreifer flüchtig, nachdem sie sich der eskortierten Werte ganz oder teilweise bemächtigt haben, kann das Feuer auf sie oder ihre Fahrzeuge ohne Aufforderung eröffnet werden.

Art. 7. Die Bestimmungen der Artikel 1 bis 4 und 6 sind ebenfalls anwendbar auf den Gebrauch von Tränengas und Wasserwerfern.

Art. 8. Im Rahmen ihrer Kontroll- und Fahndungsoperationen können die in Artikel 1 erwähnten Beamten, ob von Amts wegen oder auf Befehl ihrer Vorgesetzten, oder auf Anordnung der Gerichtsbehörden, Fahrzeuge aller Art mittels Kabeln, Sturmeggen, Eisenspitzen, Sperren, Netzen und ähnlichen Vorrichtungen zum Stillstand bringen.

Art. 9. (…)

Art. 10. Wenn, in Ausübung seiner Dienstpflicht, ein Mitglied der öffentlichen Macht von seinem Vorgesetzten den Befehl erhalten hat, die Waffen oder irgendein Zwangsmittel zu gebrauchen, so ist dieser Befehl auszuführen, es sei denn er betreffe nicht die Ausübung der Dienstpflicht.
Der Befehl darf nicht ausgeführt werden, wenn seine Ausführung ein Verbrechen oder ein Vergehen darstellen würde.

Wenn in diesem Falle der Befehl trotzdem ausgeführt wird, so ist der ausführende Beamte nur dann verantwortlich, wenn er gewusst hat, oder den Umständen nach wissen konnte, dass es sich offensichtlich um ein Verbrechen oder Vergehen handelte.
Der ausführende Beamte muss, wenn die Umstände es ihm erlauben, dem Urheber des Befehls gegenüber seine Einwendungen bezüglich der Gesetzmäßigkeit des erhaltenen Befehls geltend machen.

Art. 11. Gegenwärtiges Gesetz beeinträchtigt weder die gesetzlichen Bestimmungen betreffend das Recht zur Notwehr, noch die Bestimmungen besonderer Gesetze, welche in gewissen Fällen Beamten die Anwendung von Zwangsmitteln oder den Gebrauch von Waffen in weiterem Sinne erlauben.
(…)

3. A büntetőeljárásról szóló törvény 43. Cikke szerinti speciális eset

E Cikk szerint bárki, aki valakit bűncselekmény vagy szabadságvesztéssel büntetendő cselekmény elkövetésén tettenér, megállíthatja az elkövetőt, és a legközelebbi rendőrnek átadhatja. A Szerződés 24. és 25. Cikke szerint Luxemburg területén lévő külföldi rendőrnek ugyanazok a jogai, mint bárkinek, ha a Szerződés 24. Cikk (3) és 25. Cikk (3) bekezdésének utolsó mondata szerint cselekszik.

HOLLANDIA

Hollandia nem ír elő semmilyen korlátozást a szolgálati fegyverek, kényszerítő eszközök és más felszerelés szállításra (feltéve, hogy ezeket a munkáltató adta ki).

A Szerződés 28. Cikk (2) bekezdése az alábbi jogszabály alól kivételt képez. A 2. Mellékletben felsorolt fegyverek, lőszerek és felszerelés (Hollandia esetében: lőfegyverek, paprika-spray és könnygáz) használata csak a tiszt saját magára vagy más személyre vonatkozó jogos védelme esetén megengedett (a büntető törvénykönyv önvédelemről szóló 41. Cikke). Ugyanitt arról is rendelkeznek, hogy egyedi esetben a parancsnok másként is határozhat.

1993. évi rendőrségi törvény

8. Cikk

-1. A rendőri feladat ellátásával megbízott rendőrtiszt munkája jogszerű végzéséhez erőt alkalmazhat, ha az elérendő cél ezt igazolja, figyelembe véve az erő alkalmazásából eredő kockázatokat, és feltéve, hogy a cél másképp nem érhető el. Ha lehetséges, az erő alkalmazását figyelmeztetésnek kell megelőznie.

-2. A rendőri feladat ellátásával megbízott rendőrtiszt minden helyszínre beléphet, amennyiben ez ésszerűen szükséges a segítségre szorulók megsegítéséhez.

-3. A rendőri feladat ellátásával megbízott rendőrtiszt átkutathatja egy személy ruházatát, a törvény által rászabott feladat végrehajtása közben, ha a tények vagy körülmények arra utalnak, hogy a személy, a tiszt illetve harmadik személyek élete vagy biztonsága közvetlen veszélyben van, és ez az átkutatás szükséges a veszély elhárításához.

-4. A kerületi ügyésznek vagy helyettesének, akik elé a fogvatartottakat, vagy szabadságuktól megfosztott gyanúsítottakat állítják, joguk van úgy rendelkezni, hogy ezt a személyt átkutatják, ha a tények vagy körülmények arra utalnak, hogy a személy vagy a tiszt élete vagy biztonsága közvetlen veszélyben van, és ez az átkutatás szükséges a veszély elhárításához

-5. Az 1-4. bekezdésekben említett jogok gyakorlása ésszerű és az elérni kívánt céllal arányos kell, hogy legyen.

-6. Az 1-5. bekezdések a katonai rendőrség tagjaira is vonatkoznak, ha feladatukat jogszerűen végzik, valamint a rendőrséget e törvény alapján segítő minden fegyveres erő tagjaira.

-7. Az igazságügyi miniszter előírhatja, hogy a büntetőeljárásról szóló törvény 142. Cikk 1. bekezdésében említett különleges nyomozók az 1. és 3. bekezdésben leírt jogokat gyakorolhatják, amennyiben a miniszter személyesen, kategóriánként vagy egységenként erre felhatalmazza őket. Ebben az esetben a 9. Cikk szerint egy hivatalos utasítást kell részükre adni.

9. Cikk

-1. Az igazságügyi miniszter és a belügyminiszter, valamint a honvédelmi miniszter (ha a katonai rendőrségről van szó) javaslatára egy tanácsi rendelettel a rendőrségnek és a katonai rendőrségnek hivatalos utasítást kell adni.

-2. Ha a fegyveres erők bármely más részének tagja az 59. és 60. Cikkben leírt feladatait végzi, a hivatalos utasítás alkalmazandó.

-3. A hivatalos utasítás rögzíti a 7. és 8. Cikk végrehajtásának szabályait.

-4. A tanácsi rendelettel, vagy ez alapján miniszteri rendeletben kell rendelkezni a szabadságuktól jogszerűen megfosztott személyekre alkalmazható intézkedésekről, fogvatartásuk vonatkozásában, amennyiben ez saját maguk vagy mások biztonsága érdekében szükséges. A tanácsi rendeletet az igazságügyi miniszter és a belügyminiszter, valamint a honvédelmi miniszter (ha a katonai rendőrségről van szó) javaslatára kell meghozni.

-5. A 4. bekezdés *mutatis mutandis* vonatkozik a rendőri vagy katonai őrizetbe vett személyekre is, a nekik nyújtott támogatás vonatkozásában.

-6. Az igazságügyi miniszter által a szabadságuktól jogszerűen megfosztott személyek szállítására kijelölt tisztek a 8. Cikk 1. és 3. bekezdésében említett jogokat gyakorolhatják, vagy a 4. bekezdésben említett intézkedéseket hozhatják, amennyiben ez szükséges a szállított személy szökésének

megakadályozásához. Az első teljes mondat alkalmazandó, ha a szabadságuktól jogszerűen megfosztott személyek a rendőrség vagy a katonai rendőrség őrizetében vannak.

1994. április 8-i határozat a rendőrség, katonai rendőrség és a különleges nyomozók új szolgálati szabályzatáról és a szabadságuktól jogszerűen megfosztott személyekkel szemben megtehető intézkedésekről (Hivatalos Utasítás a rendőrség, katonai rendőrség és a különleges nyomozók számára [2006. szeptember 20-tól hatályos változat])

Megjelent: Staatsblad 1994, 825; Staatsblad 1997, 764; Staatsblad 1998, 340; Staatsblad 1999, 197; Staatsblad 2001, 387; Staatsblad 2002, 174; Staatsblad 2004, 218; Staatsblad 2005, 110; Staatsblad 2006, 407

Mi Beatrix, Isten kegyelméből Hollandia királynője, Orange-Nassau hercegnője, stb., stb., stb.

Az igazságügyi és a belügyminiszter javaslatára, a honvédelmi miniszter egyetértésével;

az 1993. évi rendőrségi törvény 9. cikkére tekintettel;

az államtanács véleményének figyelembevételével (1994. március 28., no. W.O. 3.93.0838);

Az igazságügyi miniszter további jelentésének fényében, amelyet belügyminiszterünk nevében is készült, a honvédelmi miniszterrel egyetértésben kiadva;

Jóváhagytuk és megerősítettük:

1. FEJEZET Általános rendelkezések

1. Cikk

1. E rendelet alkalmazásában tiszt:

a. az 1993-as rendőrségi törvény 3. Cikk 1 a) és c) és 2) bekezdésében említett rendőrtiszt.

b. a rendőrtiszt, amennyiben az 5. fejezet 1. és 2. Cikkére vonatkozik. A rendelet 6. fejezetében tiszt alatt az 1993-as rendőrségi törvény 3. Cikk 1 b) bekezdésében említett rendőrtiszt vagy más személy értendő, amennyiben ez a tiszt vagy személy egy különleges nyomozó, és a rendőrkapitány fogvatartottak őrzésével bízta meg.

c. a gyakornoknak kinevezett személy, a gyakorlati idő alatt;

d. a katonai rendőrség tagjai rendőri feladatok végzése során, az 1993-as rendőrségi törvény 6. Cikk 1. bekezdése szerint;

e. a fegyveres erők tagjai az 1993-as rendőrségi törvény 59. Cikk 1. bekezdése és 60. Cikke értelmében;

2. Ebben a rendeletben az alábbi kifejezések az alábbi jelentést hordozzák:

a. elöljáró az a tiszt, aki feladatát végzi, vagy akit paranccsal vagy vagy utasítással ezzel megbíztak, vagy aki parancsnok.

b. ha az a. pont rendelkezései szerint nincs elöljáró, a magasabb rangú tiszt, egyenlő rangok esetén a hosszabb szolgálati idejővel rendelkező személy, a katonai rendőrség, vagy más fegyveres szervek esetén a katonai büntető törvénykönyv 67. Cikke szerint az elöljáró.

3. Ebben a rendeletben az alábbi kifejezések az alábbi jelentést hordozzák:

a. kompetens hatóság: az 1993-as rendőrségi törvény 12., 13. és 15. Cikkében említett hatóság;

b. erő: az erő minden, enyhénél nagyobb mértékű, kényszerítő jellegű alkalmazása személyek vagy tárgyak ellen;

c. erő alkalmazása: az erő alkalmazása és az ezzel való fenyegetés, beleértve egy lőfegyver kézbevételét;

d. fegyver:

1o. az 1993-as rendőrségi törvény 49. Cikk 1. bekezdése felszerelés, fegyverek és lőszerek, amelyeket erő alkalmazására lehet használni, és

2o. 6., 58., 59. és 60. Cikkében leírt rendőri feladaatok elvégzéséhze használható, a honvédelmi miniszter által engedélyezett felszerelés, fegyverek és lőszerek.

e. kitoloncolási eszközök:

1. az 1993-as rendőrségi törvény 49. Cikk 1. bekezdése alapján az idegenek kitoloncolására egy, a 2000. évi idegenrendészeti törvényi alapján határőrizetre vagy idegenek felügyeletére feljogosított rendőr által használt eszköz, és

2. az idegenek kitoloncolására egy, a 2000. évi idegenrendészeti törvényi alapján határőrizetre vagy idegenek felügyeletére feljogosított katonai rendőr által használt, a honvédelmi miniszter által a bevándorlási és integrációs miniszterrel együttesen kiadott eszköz;

f. automata lőfegyver: olyan lőfegyver, amelyből több lövés adható ki az elsütőszerkezet egy meghúzásával, vagy olyan lőfegyver, amely választás szerint egy vagy több lövést tud kiadni;

g. rohamrendőrség: a regionális rendőrségek ellenőrzéséről szóló határozat 6. Cikke szerinti rendőri egység és a hasonló feladattal megbízott katonai rendőrségi egység, az előbb említett határozat szerint;

h. orvos: a szolgálatban lévő orvos;

i. különleges nyomozó: a büntetőeljárásról szóló törvény 142. Cikk 1. bekezdésében említett különleges nyomozó;

j. lőfegyver használata: ráfogni valakire, ráfogva tartani vagy ténylegesen használni egy lőfegyvert;

k. nem behatoló lőszer: lőszer, amit úgy terveztek, hogy ne hatoljon be az eltalált személy testébe.

4. Ebben a rendeletben fogvatartott alatt a szabadságától jogszerűen megfosztott személy értendő, vagy az, akit egy rendőrségi fogdában őriznek, a neki nyújtott segítség vonatkozásában

2. Cikk

A tisztnek részére kiállított igazolvánnyal kell magát azonosítania:

a. ha civil ruhában dolgozik, anélkül, hogy erre felkérnék, kivéve ha különleges körülmények ezt lehetetlenné tesszik, és

b. egyenruhában dolgozva kérésre.

3. Cikk

Az 1993-as rendőrségi törvény IX. Fejezete szerint segítséget nyújtó tiszt a helyi kompetens hatóság irányítása alá tartozik, vagy az e hatóság által kijelölt tiszt alá.

2. FEJEZET Erő

1. § Általános rendelkezések

4. Cikk

A tiszt csak akkor használhatja fegyverét, ha:

a. ez jogszerűen áll rendelkezésére, amennyiben olyan feladatot végez, amihez azt kapta, és

b. aki jártas ennek a fegyvernek a használatában.

5. Cikk

1. Ha a tiszt egy lezárt területen vagy máshol egy jelen lévő felettes irányítása alatt cselekszik, csak akkor használhat erőt, ha erre a felettes kifejezetten utasította. A felettesnek kell jeleznie, hogy melyik fegyvert kell használni.

2. Az 1. bekezdés nem alkalmazandó akkor, ha az 1. bekezdésben említett felettes előzetesen másként rendelkezett.

3. Az 1. bekezdés akkor sem alkalmazandó, ha a 10. Cikk 11.b bekezdése szerinti helyzet áll fenn, amennyiben nem lett volna ésszerű megvárni a parancsot.

6. Cikk

1. A rendőrkapitány, vagy az általa kijelölt tiszt csak akkor vetheti be a regionális rendőrségek ellenőrzéséről szóló határozat 6. és 8. cikke szerinti egységeket, ha a kompetens hatóság beleegyezett.

2. A kompetens hatóság által kijelölt tiszt az 1993-as rendőrségi törvény 58. és 59. Cikkében említett egységeket csak a kompetens hatóság beleegyezését követően vetheti be.

2. § Lőfegyverek

7. Cikk

1. A lőfegyver – amely nem automata fegyver vagy nagy hatótávolságú precíziós fegyver – használata csak akkor megengedett, ha:

a. olyan személy elfogására, akiről okkal feltételezhető, hogy lőfegyver van nála, amit azonnal használni tud, és azt emberek ellen kívánja irányítani;

b. olyan személyt kell feltartóztatni, aki megszökött, vagy megkísérelt megszökni a fogvatartásból, vagy más szabadságvesztésből, és akit olyan bűncselekmény elkövetése miatt gyanúsítanak vagy ítéltek el

1°. Ami négy vagy több év börtönbüntetéssel sújtható, és

2°. Ami a testi épség vagy személyi szabadság súlyos megsértését okozza, vagy

3°. Aminek következményei a társadalomra veszélyesek.

c. a zavargás vagy más súlyos rendbontás letörésére, ha a kompetens hatóság erre parancsot adott és lezárt területen egy felettes felügyelete melletti műveletben történik;

d. katonai zavargás vagy más súlyos katonai rendbontás vagy lázadás letörésére, ha a katonai rendőrség tagjai a honvédelmi miniszter vagy a katonai ügyekkel megbízott arnhemi ügyész utasítására cselekszenek egy lezárt területen egy felettes felügyelete mellett.

2. fegyverhasználat az 1. bekezdés a és b pontjai esetében csak személyek és olyan szállító járművek ellen megengedett, amelyekben vagy amelyeken emberek vannak.

3. Az 1 bekezdés a és b pontjában írt esetekben nem használható lőfegyver, ha az elfogandó személy azonossága ismert, és okkal feltételezhető, hogy az elfogás elhalasztása nem jelent a közbiztonságra elfogadhatatlan kockázatot.
4. Az 1. bekezdés b pontjában említett bűncselekmény elkövetésébe beletartozik a kísérlet és a büntető törvénykönyv 47. és 48. Cikkében leírt részesi formák.

8. Cikk

1. Az automata lőfegyver használata csak akkor megengedett, ha személyek és olyan szállító járművek ellen irányul, amelyekben vagy amelyeken emberek vannak, olyan helyzetben, amikor valaki saját maga vagy más testi épségét közvetlenül és jogtalanul veszélyezteti.
2. Automata lőfegyvert csak oktatási célból, vagy az alábbi esetekben lehet viselni:
a. egy olyan személy elfogása során, akiről okkal felételezhető, hogy lőfegyver van nála, amely azonnal használható, és ezt emberek ellen fogja használni.
b. emberek és tárgyak őrzésére és biztoosítására.
3. Automata lőfegyvereknek a 2. bekezdés a pontjában említett szállítása csak a kerületi ügyész beleegyezésével, és az igazságügyi miniszter írásos engedélyével lehetséges. Az engedélyt írásban kell kérni a *College van procureurs-generaal*–on keresztül. Ha az engedélyt nem lehet írásban kérni vagy megadni a sürgősség miatt, az engedélyt szóban is lehet kérni, illetve megadni. A szóbeli engedélyt 24 órán belül írásban is meg kell erősíteni. Ha lehetséges, a kerületi ügyész az érintett polgármestert az automata lőfegyverek szállításáról előre értesíti.
4. A 2. bekezdés b pontja szerinti lőfegyver-szállítás csak a kompetens hatóság belegyezését követően és az igazságügyi és a belügyminiszter közös írásos engedélyének megadása után lehetséges. A kompetens hatóságnak az engedélyt írásban kell kérnie. Ha az engedélyt nem lehet írásban kérni vagy megadni a sürgősség miatt, az engedélyt szóban is lehet kérni, illetve megadni. A szóbeli engedélyt 24 órán belül írásban is meg kell erősíteni.

9. Cikk

1. Egy nagy hatótávolságú precíziós fegyver használata csak nagyon súlyos bűncselekmény esetén, az emberek életét fenyegető közvetlen veszély esetén megengedett.
2. Az 1. bekezdésben említett fegyver használata csak a regionális rendőrségek ellenőrzéséről szóló rendelet 9. Cikkében, vagy az 1993-as rendőrségi törvény 60. Cikkében leírt speciális egység (*bijstandseenheid*) parancsnokának utasítására történhet.
3. A nagy hatótávolságú precíziós fegyvert csak oktatásra, vagy a nagyon súlyos bűncselekmények tényleges leküzdésére lehet viselni, amennyiben a körülmények közvetlen életveszélyre utalnak.
4. A nagy hatótávolságú precíziós fegyver szállítása súlyos bűncselekmények elleni tényleges fellépéshez, amelyek közvetlen életveszélyt jelentenek, csak a kompetens hatóság belegyezését követően lehetséges és az igazságügyi miniszter írásos engedélyével. Az engedély megadása feltételekhez köthető. Ha az engedélyt nem lehet írásban kérni vagy megadni a sürgősség miatt, az engedélyt szóban is lehet kérni, illetve megadni. A szóbeli engedélyt 24 órán belül írásban is meg kell erősíteni.

10. Cikk

1. A tiszt csak akkor vehet kézbe lőfegyvert – ami nem automata és nem nagy hatótávolságú, precíziós:
a. amikor a lőfegyver használata megengedett, vagy
b.biztonságával vagy mások biztonságával kapcsolatban, ha okkal feltételezhető, hogy olyan helyzet áll elő, amikor jogosult lőfegyvert használni.
2. Ha nem állt elő az 1.b szerinti helyzet, vagy megszűnt, a tisztnek rögtön el kell tennie a lőfegyvert.

10a. Cikk

1. A tisztnek lőfegyver (ami nem automata s nem nagy hatótávolságú, precíziós) célra emelése és elsütése előtt közvetlenül figyelmeztetést kell adnia, hangos szóval vagy más félreérthetetlen módon, hogy ha nem követik a parancsot, lőni fog. Ezt a figyelmeztetést, amit szükség esetén egy figyelmeztető lövés helyettesíthet, nem kell elvégezni, ha a körülmények nem engedik meg.
2. A figyelmeztető lövést amennyire csak lehet, úgy kell leadni, hogy az emberekre vagy tárgyakra a legkisebb veszélyt jelentse.

2a. § Nem behatoló lőszer

11. Cikk

A 7-10a Cikkek nem alkalmazandóak a nem behatoló lőszerrel töltött lőfegyverek használatára vagy kezelésére.

11a. Cikk

A nem behatoló lőszerrel töltött lőfegyver használata csak akkor megengedett, ha:
a. olyan személy elfogására, akiről okkal feltételezhető, hogy lőfegyver van nála, amit azonnal használni tud, és azt emberek ellen kívánja irányítani;
b. olyan személyt kell feltartóztatni, aki megszökött, vagy megkísérelt megszökni a fogvatartásból, vagy más szabadságvesztésből, és akit egy bűncselekmény elkövetésével gyanúsítanak vagy elítéltek

11b. Cikk

A tisztnek a nem behatoló lőszerrel töltött lőfegyver célra emelése és elsütése előtt közvetlenül figyelmeztetést kell adnia, hangos szóval vagy más féleérthetetlen módon, hogy ha nem követik a parancsot, lőni fog. Ezt a figyelmeztetést, amit szükség esetén egy figyelmeztető lövés helyettesíthet, nem kell elvégezni, ha a körülmények nem engedik meg.

11c. Cikk

A 11a. és 11b. Cikk mutatis mutandis alkalmazandó, ha a nem behatoló lőszert nem lőfegyverből lövik ki.

2b. § Paprika-spray

12a. Cikk

1. A paprika-spray csak akkor megengedett, ha:
a. olyan személyt kell elfogni, akiről okkal feltételezhető, hogy lőfegyver van nála, amit azonnal használni tud, és azt emberek ellen kívánja irányítani;
b. olyan személyt kell feltartóztatni, aki megszökött, vagy megkísérelt megszökni a fogvatartásból, vagy más szabadságvesztésből, és akit egy bűncselekmény elkövetésével gyanúsítanak vagy elítéltek
c. agresszív állatok elleni védekezésre vagy ezek megfékezésére.
2. a parikaspray nem használható:
a. láthatóan 12 évnél fiatalabb vagy 65 évnél idősebb személy ellen;

b. láthatóan terhes nő ellen;
c. olyan személyek ellen, akiknek aránytalanul nagy sérülést okozna, pl. légzőszervi megbetegedések miatt, amik a tiszt számára láthatóak.
d. csoportok ellen.

12b. Cikk

A tisztnek a paprikaspray célra emelése és használata előtt közvetlenül figyelmeztetést kell adnia, hangos szóval vagy más félreérthetetlen módon, hogy ha nem követik a parancsot, sprayt fog használni. Ezt a figyelmeztetést nem kell elvégezni, ha a körülmények nem engedik meg.

12c. Cikk

A paprikasprayt legfeljebb kétszer lehet egy személy ellen használni, legfeljebb 1 másodpercig és legalább egy méterről.

3. § Más fegyverek

13. Cikk

1. A CS könnygáz használata csak akkor megengedett. ha:
a. zárt területen olyan személy elfogására, akiről okkal feltételezhető, hogy lőfegyver van nála, amit azonnal használni tud, és azt emberek ellen kívánja irányítani;
b. nem zárt területen közvelen veszélyt jelentő tömeg oszlatására
2. A CS könnygáz használata csak a felettes utasítására, a kompetens hatóság beleegyezésével történhet.
3. Az ezt elrendelő felettes meghatározza a használandó CS könnygázgránátok számát.

14. Cikk

A vízágyú használata csak akkor megengedett, ha a bevetési egység a felettes utasítására cselekszik, és megkapta a kompetens hatóság belegyezését.

15. Cikk

1. A rendőrkutya használata csak gazdájának közvetlen és folyamatos felügyelete mellett lehetséges.
a. az őrjárat során és
b. a bevetési egység akciójában a kompetens hatóság beleegyezését követően.
2. A gazdának az 1993-as rendőrségi törvény 49. Cikk 1. bekezdése szerinti tanúsítvánnyal kell rendelkeznie.

16. Cikk

Az elektromos sokkoló használata csak aggresszív állatok ellen engedhető meg, a felettes beleegyezését követően.

4. § Az erő alkalmazásának jelentése

17. Cikk

1. A tisztnek, aki erőt alkalmazott, azonnal jelentenie kell a megfelelő körülményeket, valamint tettének következményeit a felettesének.
2. A felettes azonnal rögzíti a jelentést az igazságügyi és a belügyminiszter által rendeletben megállapított módon.
3. A rendőrkapitány a 2. bekezdésben említett jelentést 48 órán belül eljuttatja a kerületi ügyésznek, vagy a katonai rendőrség parancsnokának, ha
a. az erő alkalmazásának következményei erre okot adnak,
b. az erő alkalmazása testi sérülést okozott, vagy halálhoz vezetett,
c. lőfegyvert használtak.

18. Cikk

[hatályon kívül helyezve.]

19. Cikk

A felettesnek amint lehet, tájékoztatnia kell a tisztet a jelentésről. A tiszt kérésére ideiglenes tájékoztatást is lehet adni.

3. FEJEZET Ruházat átkutatása

20. Cikk

1. Az 1993-as rendőrségi törvény 8. Cikk 3. bekezdésében hivatkozott átkutatás a ruha felületén át kell, hogy történjen, és ha lehet, az átkutatott személlyel megegyező nemű tiszt által végzendő.
2. Az 1993-as rendőrségi törvény 8. Cikk 4. bekezdésében hivatkozott átkutatást az átkutatott személlyel megegyező nemű tisztnek kell végeznie.

21. Cikk

Az 1993-as rendőrségi törvény 8. Cikk 3. vagy 4. bekezdésében hivatkozott átkutatást végző tiszt azonnal írásban jelenti felettesének ezt, megjelölve az okokat.

4. FEJEZET Bilincs

22. Cikk

1. A tiszt a szabadságától jogszerűen megfosztott személyen szállítás céljából helyezhet el bilincset.
2. Az 1. bekezdésben leírt intézkedés csak olyan körülmények közt megengedett, amikor a szökés veszélye vagy személyek testi épségének károsodása fennáll.
3. A 2. bekezdésben leírt körülmények csak az alábbiakra vonatkozhatnak:
a. a szabadságától jogszerűen megfosztott személyre vagy
b. a bűncselekmény fajtájára, ami miatt megfosztották szabadságától.

23. Cikk

A 22. cikkben említett bilincset használó tiszt erről azonnal írásban értesíti felettesét, leírva az okokat.

4A. FEJEZET Idegenek kitoloncolásának eszközei

23a. Cikk

1. A 2000-es idegenrendészeti törvény értelmében a tiszt korlátozhatja az idegenek szabad mozgását repülőgéppel történő kitoloncolásakor, a kitoloncolás megfelelő végrehajtása érdekében.
2. Az 1. bekezdésben említett intézkedést csak akkor lehet megtenni, ha:
a. fennáll a szökés veszélye, az idegen, a tiszt vagy harmadik személy életének vagy biztonságának vagy a közrend komoly megzavarásának veszélye, és
b. az nem kockáztatja az idegen egészségét
3. Ha az 1. bekezdésben említett tiszt egy jelen lévő felettes felügyelete mellett jár el, csak kifejezett parancsra cselekedhet így. A felettesnek jeleznie kell a használandó eszközöket.
4. Csak az eszköz használatában jártas tiszt járhat el így.

23b. Cikk

1. A 23a Cikk 1. bekezdésében leírt cselekményt véghezvivő tiszt erről azonnal írásos jelentést készít felettesének, megnevezve az okokat és a következményeket.
2. A felettes az 1. bekezdésben leírt jelentésről feljegyzést készít.

5. FEJEZET Segítségnyújtás

24. Cikk

1. A tiszt gondoskodik arról, hogy a könnyebben sérült, betegség tüneteit mutató vagy erre kétségkívül rászoruló személyek orvoshoz kerüljenek, vagy kórházba, és ha kell, gondoskodik szállításukról
2. A tiszt gondoskodik arról, hogy a súlyosan sérült vagy öntudatlan személyek (ideértve azokat is, akiket nem lehet felébreszteni vagy zavartan viselkednek) mentők révén kórházba kerüljenek. A tisztnek az egészségügyi személyzet számára tájékoztatást kell adnia az állapotot kiváltó okokról és a személynél talált gyógyszerekről.

25. Cikk

1. A tisztnek biztosítania kell, hogy az alkoholos befolyás alatt álló személyek, vagy más miatt a közrendre, -egészségre, -biztonságra vagy önmagukra közvetlen veszélyt jelentő személyeket a leginkább megfelelő módon eltávolítsa a közterületről a gyülekezési törvény 1. Cikke szerint. Közterületnek minősülnek a közterületen elhelyezett szállítójárművek is, amennyiben ezek nem lakhatási célt szolgálnak.
2. A tiszt átadja az 1. bekezdésben említett személyeket a megfelelő szociális intézménynek, ha erre lehetőség van. Ha nincs megfelelő gondodkodást nyújtó létesítmény máshol, ezek a személyek segítségnyújtás keretében a rendőrségen is elhelyezhetőek, ha ez védelmükhöz szükséges, és nem akaratuk ellen való.
3. A tiszt orvost hív az 1. bekezdésben írt, mentálisan zavart vagy ilyennek tűnő személyhez, miután megkísérelte elérni annak háziorvosát.

6. FEJEZET Fogvatartottakkal szembeni intézkedések

1. § Általános rendelkezések

26. Cikk

1. A tiszt a fogvatartottat a regionális rendőrségek ellenőrzéséről szóló határozat 15. Cikke szerint kezeli.
2. A tiszt a a regionális rendőrségek ellenőrzéséről szóló határozat 15. Cikk 6. bekezdése szerint lejegyzi a részleteket.

27. Cikk

1. Ha nem ellentétes a büntetőeljárásról szóló törvénnyel, a tiszt tájékoztatja a fogvatartott családtagját vagy élettársát a bebörtönzésről. Ha nagykorú, ebbe a fogvatartottnak előzetesen bele kell egyeznie.
2. Ha a körülmények nem teszik lehetővé az 1. bekezdésben leírtakat, a nem rezidens fogvatartott esetén ennek nagykövetségét vagy konzulátusát kell értesíteni.

2. § Ruha és tárgyak elvétele

28. Cikk

1. A tiszt átkutathatja a fogvatartottat és ruháját veszélyt okozó tárgyakat keresve.
2. Ha a tiszt az 1. bekezdésben említett tárgyakat talál, ezeket le kell foglalnia.
3. Az 1. bekezdésben említett kutatás ha lehet, a fogvatartottal azonos nemű tiszt által kell, hogy történjen.

29. Cikk

1. A tiszt csak akkor kérheti a fogvatartottat ruhái levetésére, ha:
a. a bebörtönzés során a ruha veszélyt jelenthet a fogvatartott vagy mások biztonságára, és a kerületi ügyész ebbe beleegyezett;
b. az orvos véleménye szerint a bebörtönzés során a ruha veszélyt jelenthet a fogvatartott vagy mások biztonságára;
2. A tisztnek meg kell őriznie az 1. bekezdésben említett ruhákat és gondoskodnia kell pótlásukról.

30. Cikk

1. A 28. Cikk 1. bekezdésében említett kutatást végző tiszt azonnal írásos jelentést készít erről felettesének
2. A tiszt precízen feljegyez minden, megőrzésre átvett dolgot. A kis méretű értékek és tárgyak esetén elég egy általános leírás.
3. A 2. bekezdésben írt feljegyzés egy példányát a fogvatartottnak és a tisztnek kell aláírnia, és át kell adni a fogvatartottnak.

3. § Állandó videófelügyelet

31. Cikk

1. A kerületi ügyész helyettesének beleegyezését követően a tiszt a fogvatartottat állandó videófelügyelet alá helyezheti.
2. Az 1. bekezdésben említett intézkedések csak abban az esetben megengedettek, ha az életet vagy a biztonságot fenyegető veszély áll fenn, és ezért folyamatos megfigyelés szükséges.
3. A tisztnek tájékoztatnia kell a személyt az állandó videófelügyeletről, és rögzíteni kell azt.

4. § Orvosi segítségnyújtás

32. Cikk

1. Amennyiben van arra utaló jel, hogy egy fogvatartottnak orvosi segítségnyújtásra van szüksége, vagy gyógyszereket találtak ennél a személynél, a tisztnek konzultálnia kell az orvossal. A tisztnek akkor is konzultálnia kell az orvossal, ha maga a fogvatartott kér orvosi segítséget, vagy gyógyszert.
2. Ha a fogvatartott saját orvosától kér segítséget, a tisztnek erről tájékoztatnia kell az orvost.
3. Ha a fogvatartott jelzi, hogy nem kér orvosi segítséget, miközben vannak arra utaló jelek, hogy erre szüksége lenne, a tiszt tájékoztatja az orvost erről.

33. Cikk

A tiszt nem korlátozhatja a orvost a vizsgálatban és a kezelésben. Követnie kell az orvos utasításait a fogvatartott gondozása során, és le kell jegyeznie az orvos által adott utasításokat.

34. Cikk

1. A tisztnek rendszeresen meg kell vizsgálnia a fogvatartottat,az alábbiak szerint:
a) a fogvatartottat cellájában legalább 15 percenként ellenőrizni kell, amennyiben orvost hívtak hozzá;
b) ha már megadták az orvosi segítséget, a fogvatartottat olyan gyakran kell ellenőrizni, ahogy azt az orvos előírta;
c) ha nincs szükség orvosi beavatkozásra, a fogvatartottat két óránként kell ellenőrizni.
2. Az 1.a) és b) pontban hivatkozott esetekben a tisztnek ellenőriznie kell a cellát és a személyt, különösen azt, hogy a fogvatartott milyen mértékben ébreszthető fel és zavartan viselkedik-e. Ha nem ébreszthető fel egy személy, vagy zavartan viselkedik, azonnal kórházba kell szállítani.
3. A tisztnek rögzítenie kell az 1. bekezdés alapján tett megfigyeléseit.

35. Cikk

A fogvatartott szállítása során a tisztnek a 26. Cikk 2. bekezdése, 33. Cikk és 34. Cikk 3. bekezdése szerinti gyógyszereket és okmányokat magával kell vinnie, ha ezek relevánsak lehetnek, és az orvosi jelentéseket, amelyeket a fogvatartott kezelését átvevő orvosnak szántak.

5. § Szabadon engedés

36. Cikk

A tiszt gondoskodik arról, hogy a szabadon engedett személy az általa megjelölt helyre szállítsák.

7. FEJEZET Különleges nyomozó

37. Cikk

1. Ha az igazságügyi miniszter az 1993-as rendőrségi törvény 8. Cikk 7. bekezdése szerint úgy rendelkezett, hogy egy különleges nyomozónak joga van ezen Cikk 1. és 3. bekezdésében leírt jogokat gyakorolni, akkor ezen határozat 5, 17, 19. Cikk, 20. Cikk 1. bekezdés és 21. Cikke szerint járhat el. A 17. Cikk 3. bekezdésében írt „kapitány" felettest jelent.
2. Ha a parancs fegyver, kutya vagy bilincs használatára is kiterjed, a különleges nyomozó e határozat 4. Cikke, 7. Cikk 1. bekezdés *a* és *b*, 2, 3 és 4 bekezdés, 10, 10a, 12a, 12b, 12c Cikkei, 15. Cikk 1. bekezdés *a* és 2. bekezdés, 16. 22. és 23. Cikkek szerint jár el.
3. Az 1. és 2. bekezdés alkalmazásában az alábbi kifejezések az alábbi jelentést hordozzák:
a. kompetens hatóság: az 1993. évi rendőrségi törvény 13. Cikkében említett hatóság;
b. elöljáró: a közvetlen elöljáró, a különleges nyomozókról sszóló határozat 1. Cikke szerint.
c. fegyver: fegyverek, lőszerek és felszerelés, amit erő kifejtésére lehet használni, a fegyverekről és lőszerekről szóló törvény 3a Cikk 1-3. bekezdései alapján.

38. Cikk

Fegyverek vagy bilincs használatára feljogosított különleges nyomozók a fegyvereket vagy bilincseket csak az igazságügyi miniszter által előírtaknak megfelelően használhatják feladatuk végzése során.

39. Cikk

A különleges nyomozók nem gyakorolhatják az 1993-as rendőrségi törvényben leírt jogokat, amíg esküt nem tettek, és a tiszt tanúbizonyságot nem tett szakértelméről.

8. FEJEZET Záró rendelkezések

39a. Cikk

Az igazságügyi miniszterrel egyetértésben a rendőrség, a katonai rendőrség, és a különleges nyomozók szolgálati szabályzatának a nem behatoló lövedékekkel kapcsolatos módosításáról szóló 2006. augusztus 25-i rendelet (Stb. 2006, 407) hatálybalépését követően három éven belül a belügyminiszter egy jelentést ad a parlamentnek a 11-11c Cikkek gyakorlati tapasztalatairól.

40. Cikk

Ez a határozat az 1993-as rendőrségi törvény hatályba lépésének napján lép hatályba.

41. Cikk

Erre a határozatra a „Rendőr-, katonai rendőr- és különleges nyomozótisztek hivatali szabályzata" néven kell hivatkozni.

Ezt a határozatot és magyarázatát a *Staatsblad* közlönyben kell közzétenni.

Hága, 1994. április 8.

Beatrix

E. M. H. Hirsch Ballin
igazságügyi miniszter

E. van Thijn
belügyminiszter

közzétéve 1994. április huszonegyedikén
E. M. H. Hirsch Ballin
igazságügyi miniszter

SPANYOLORSZÁG

Spanyolország engedélyezte a többi prümi Fél rendőrségeinek a közös műveletek során, vagy sürgős helyzetekben a szokásos felszerelés használatát. Ha a felszerelés ettől nagymértékben eltér, kötelező a külön engedélyeztetés.

A Szerződés 5. és 6. fejezete általános elvként a fogadó ország nemzeti jogának fennhatóságát állapította meg, a Schengeni Egyezmény végrehajtási megállapodásának 43. Cikke (a Szerződés 30. Cikke) szerinti felelősségi rendszer analógiájára, és a Szerződés 25. Cikk (5) bekezdése szerinti fogadó állam által viselt felelősségre tekintettel.

Ha a spanyol rendőrök számára egyes fegyverek szállítása vagy használata jogi akadályokba ütközik, ugyanezek a korlátozások érvényesek más Felek spanyol területen fellépő rendőreire. A spanyol nemzeti jog szerint

1.- Mindenki – civilek és rendőrök – számára egyaránt szigorúan tilos az alábbi típusú fegyverek birtoklása és használata:

a. Azon fegyverek, amelyek tulajdonságait engedély nélkül jelentősen megváltoztatták.
b. A zárszerkezetükben, vagy tárukban speciális szerkezeteket tartalmazó puskák
c. A kis zárszerkezettel felszerelt puskák és pisztolyok.
d. A botot vagy más tárgyat tartalmazó lőfegyverek.
e. A bármely más tárgynak álcázott lőfegyverek.
f. A hosszú kardok, bármely típusú tőrök és az automata kések. A 11 centiméternél kisebb pengéjű, kétélű, kihegyezett szúró- és vágóeszközöket tőröknek kell tekinteni.
g. A légsűrítéssel, vagy bármely más gáz sűrítésével működő, szúró- és vágóeszközökkel kombinált lőfegyverek.
h. A drótból vagy ólomból készült bot, az agyi sokkoló, a „llave de pugilato”, tüskékkel vagy anélkül, a csúzli és a fújócső, a „munchaco” és a „xiriquete”, valamint bármely más, a személyek testi épségét veszélyeztető eszköz.

2.- Tilosak – kivéve a szakképzett köztisztviselők (köztük a rendőrök) számára (1)

a. A 2.2. és 3.2 kategóriájú félautomata fegyverek, amelyek tárolókapacitása legfeljebb 5 golyó, amelyek zárszerkezete a fegyverházban van, vagy kivehető.

b. Az önvédelmi spray-k, és minden, gázt vagy aerosolt kibocsátó fegyver, illetve bármilyen, mérgező vagy maró hatású vegyi anyagot kibocsátani képes mechanizmussal ellátott készülék.
c. Az elektromos vagy gumibot, vagy ehhez hasonlók.
d. A lőfegyverekre szerelhető hangtompító.
e. Az átfúrt lőszereket tartalmazó töltény, robbanó vagy gyulladó golyók, valamint az ennek megfelelő lövedékek.
f. A „dumdum”- vagy „lecsiszolt végű” lövedékes puskák és pisztolyok lőszerei, és ezek saját lövedékei
g. A ferde csövű puskák.

(1) A Spanyolországban engedélyezett kaliber-, súly-, átmérő és gázjellemzőket átadtuk az elnökségnek. A jelen dokumentumban a spanyol rendőrök alapfelszerelésének vázlata jelenik meg.

3. A Spanyolország által hadifegyvernek tekintett, és ezért a rendőrök által csak a spanyol kormány engedélyével használható fegyverek:

a. 20 milliméteres vagy nagyobb kaliberű lőfegyverek vagy rendszerek.
b. 20 milliméternél kisebb kaliberű lőfegyverek vagy fegyverrendszerek, amelyek kaliberét a Honvédelmi Minisztérium katonainak sorolta be.
c. Automata lőfegyverek.
d. Az a) és b) pontban jelzett fegyverek lőszere.
e. Légi bombák, rakéták, torpedók, aknák, gránátok, valamint ezek fő alkatrészei.
f. Az előző pontokban nem felsorolt, de a Honvédelmi Minisztérium által katonainak besorolt fegyver.

AZ ÖNVÉDELEM SZABÁLYAI

Spanyolországban az tekintendő jogos védelemnek, ha valaki egy személy, vagy saját maga illetve mások jogainak védelmében cselekszik, amennyiben az alábbi követelmények fennállnak:

Személyek védelme.-

1.- Jogtalan erőszak
2.- Ennek elkerülésére vagy elhárítására alkalmazott eszköz ésszerű szükségessége
3.- A védekező részéről elegendő provokáció hiánya

Tárgyak védelme.-

Tárgyak védelme esetén jogtalan erőszaknak minősül a bűntett vagy vétség, és a tárgy rongálás vagy megsemmisülés közvetlen veszélyének van kitéve.

Ingatlan (lakóhely) védelme.-

Egy ház vagy lakás védelme során jogtalan erőszaknak minősül a jogosulatlan behatolás. Ebben az értelemben háznak minősül minden zárt terület, amit a bentlakó mások kizárásával használ.”

4. §

(1) E rendelet – a (2) bekezdésben meghatározott kivétellel – 2007. december 1-jén lép hatályba.

(2) E rendelet 3. §-a a Végrehajtási megállapodás 20.1 pontjában meghatározott időpontban lép hatályba.

(3) A Végrehajtási megállapodás és e rendelet 3. §-a hatálybalépésének naptári napját a külpolitikáért felelős miniszter annak ismertté válását követően a Magyar Közlönyben haladéktalanul közzétett egyedi határozatában állapítja meg.

Budapest, 2007. augusztus 1.

A miniszterelnök helyett:

Dr. Veres János s. k.,
pénzügyminiszter

A Magyar Közlönyt szerkeszti a Miniszterelnöki Hivatal, a Szerkesztőbizottság közreműködésével. A Szerkesztőbizottság elnöke: Gilyán György. A szerkesztésért felelős: dr. Tordai Csaba. Budapest V., Kossuth tér 1–3.
Kiadja a Magyar Hivatalos Közlönykiadó. Felelős kiadó: dr. Kodela László elnök-vezérigazgató.
Budapest VIII., Somogyi Béla u. 6., www.mhk.hu. Telefon: 266-9290.

Előfizetésben megrendelhető a Magyar Hivatalos Közlönykiadónál
Budapest VIII., Somogyi Béla u. 6., 1394 Budapest 62. Pf. 357, vagy faxon 318-6668.
Előfizetésben terjeszti a Magyar Hivatalos Közlönykiadó a FÁMA Rt. közreműködésével. Telefon: 266-6567.
Információ: tel.: 317-9999, 266-9290/245, 357 mellék.
Példányonként megvásárolható a Budapest VII., Rákóczi út 30. (bejárat a Dohány u. és Nyár u. sarkán) szám alatti Közlöny Centrumban (tel.: 321-5971, fax: 321-5275, e-mail: kozlonycentrum@mhk.hu), illetve megrendelhető a kiadó ügyfélszolgálatán (fax: 318-6668, 338-4746, e-mail: kozlonybolt@mhk.hu) vagy a www.mhk.hu/kozlonybolt internetcímen.
2007. évi éves előfizetési díj: 99 792 Ft. Egy példány ára: 210 Ft 16 oldal terjedelemig, utána +8 oldalanként +189 Ft.
A kiadó az előfizetési díj évközbeni emelésének jogát fenntartja.

HU ISSN 0076—2407

07.3635 – Nyomja a Magyar Hivatalos Közlönykiadó Lajosmizsei Nyomdája. Felelős vezető: Burján Norbert igazgató.