

Durchführungsvereinbarung

zum Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, unterzeichnet in Prüm, Deutschland, am 27. Mai 2005.

Abschnitt 1: Geltungsbereich und Definitionen

1. Geltungsbereich

Gemäß Artikel 44 des Vertrages umfasst die Durchführungsvereinbarung die Festlegung der erforderlichen Bestimmungen für die verwaltungsmäßige und technische Umsetzung und Anwendung des Vertrages.

2. Definitionen

Im Sinne dieser Durchführungsvereinbarung bedeutet

- 2.1 "Vertrag" der Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande, und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, unterzeichnet in Prüm, Deutschland, am 27. Mai 2005;
- 2.2 "Partei" eine Vertragspartei dieses Vertrags, die die vorliegende Durchführungsvereinbarung unterzeichnet hat;
- 2.3 der Vorgang des "Abrufs", des "Abgleichs" oder des "Abrufs mittels eines Vergleichs" gemäß der Artikel 3, 4 und 9 des Vertrags jenes Verfahren, mit dem festgestellt wird, ob eine Übereinstimmung der DNA-Daten oder daktyloskopischen Daten, die von einer Partei übermittelt wurden, mit den DNA-Daten oder daktyloskopischen Daten, die in den Datenbanken einer, mehrerer oder aller anderen Parteien gespeichert sind, vorliegt;
- 2.4 "DNA-Profil" ein Buchstaben- beziehungsweise Zahlencode, der eine Reihe von Identifizierungsmerkmalen des nicht codierenden Teils einer analysierten menschlichen DNA-Probe, das heißt der speziellen chemischen Form an den verschiedenen DNA-Loci, abbildet;
- 2.5 "nicht codierender Teil der DNA", die Chromosomenbereiche, die keine genetische Information, das heißt keine Hinweise auf spezifische Erbmerkmale, enthalten;
- 2.6 "DNA-Fundstellendatensatz" ein DNA-Profil und die damit verbundene Kennung;
- 2.7 der Begriff "Kennung" die Zusammenfassung folgender Elemente:
 - 2.7.1 Identifizierungscode oder eine Nummer, die es den Parteien im Fall eines Treffers ermöglicht, personenbezogene Daten und/oder Informationen aus ihren Datenbanken abzurufen, um sie gemäß Artikel 5 des Vertrags einer, mehreren oder allen Parteien zu übermitteln;
 - 2.7.2 Parteiencode, der die nationale Herkunft des DNA-Profiles anzeigt; und
 - 2.7.3 Code, der den Typ des DNA-Profiles, wie von den Parteien nach Artikel 2 Absatz 2 des Vertrags benannt, anzeigt;

- 2.8 "offene Spur" ein aus Spuren im Zuge der Ermittlung von Straftaten gewonnenes DNA-Profil einer noch nicht identifizierten Person;
- 2.9 "DNA-Personenprofil" den technischen Ausdruck für das DNA-Profil einer identifizierten Person, das in den nationalen DNA-Analyse-Dateien gemäß Artikel 2 Absatz 3 des Vertrags erfasst ist;
- 2.10 "daktyloskopische Daten" Fingerabdrücke, Fingerabdruckspuren, Handabdrücke, Handabdruckspuren und sogenannte templates derartiger Bilder (Minutien), soweit diese in einer automatisierten Datenbank gespeichert und verarbeitet werden;
- 2.11 "Folgeersuchen" ein von einer Partei an eine, mehrere oder alle anderen Parteien im Fall der Übereinstimmung vergleichener DNA-Daten oder daktyloskopischer Daten gerichtetes Ersuchen um weitere personenbezogene Daten und sonstige Informationen gemäß den Artikeln 5 und 10 des Vertrags zu erhalten;
- 2.12 "Fahrzeugregisterdatum" der im Anhang C.1 von den Parteien konkretisierte Datensatz, der in einem automatisierten Abrufverfahren gemäß Punkt 2.13 gegenseitig verfügbar gemacht wird;
- 2.13 "automatisierter Abruf" ein Online-Zugangsverfahren, um in Übereinstimmung mit Artikel 33 Absatz 1 Ziffer 2 des Vertrags auf die Datenbanken einer, mehrerer oder aller Parteien zugreifen zu können;
- 2.14 "das System gemäß Artikel 12" alle technischen Maßnahmen und funktionellen Aspekte, wie beispielsweise Netzwerk, Schnittstellen und Sicherheitsvorkehrungen, die für den Austausch von Fahrzeugregisterdaten gemäß Artikel 12 des Vertrags eingerichtet wurden;
- 2.15 "FUCARIS" „Europäisches Fahrzeug- und Führerschein-Informationssystem“, das durch Unterzeichnung des entsprechenden Vertrags am 29. Juni 2000 in Luxemburg errichtet wurde;
- 2.16 "Einzelfall" gemäß Artikel 3 Absatz 1, Artikel 9 Absatz 1 und Artikel 12 Absatz 1 des Vertrags ein einzelner Ermittlungs- oder Strafverfolgungsakt; enthält ein solcher Akt mehr als ein DNA-Profil, daktyloskopisches Datum oder Fahrzeugregisterdatum, können diese Daten gemeinsam als eine Anfrage übermittelt werden;
- 2.17 "Anlass der Anfrage oder Übermittlung von Daten" für die Anwendung des Artikels 39 des Vertrags ein Hinweis auf die eindeutige Zuordnung einer bestimmten Anfrage zum dazugehörigen Einzelfall, der Anlass für diese Anfrage war;
- 2.18 "TESTA II Kommunikationsnetzwerk" „Trans European Services for Telematics between Administrations“, ein von der Europäischen Kommission geführtes Netzwerk, sowie dessen geänderte Versionen.

Abschnitt 2: DNA-Profile

3. Zusammensetzung und Vergleich der DNA-Profile

- 3.1 Zum Zweck der Umsetzung des Artikels 2 des Vertrags bestehen die Fundstellendatensätze, die gemäß den Bestimmungen des Vertrags ausgetauscht werden, aus einem DNA-Profil und einer Kennung.
- 3.2 Eine Zusammenstellung genereller technischer Spezifikationen, einschließlich der Abgleichsregeln, der Algorithmen und der Parteiencodes gemäß der Definitionen in den Anhängen A., wird durch die nationalen Kontaktstellen der Parteien eingeführt und umgesetzt und bei allen Anfragen und Antworten bezüglich der Abrufe und Abgleiche von DNA-Profilen gemäß Punkt 3.1 eingesetzt.
- 3.3 Der Vergleich der DNA-Profile erfolgt auf Grundlage der im Anhang A.1 bestimmten gemeinsamen Markern. Jedes von der anfragenden Partei zum automatisierten Abruf oder Abgleich übermittelte DNA-Profil wird mit allen von der angefragten Partei in Übereinstimmung mit Artikel 2 Absätze 2 und 3 des Vertrags zur Verfügung gestellten DNA-Profilen verglichen.
- 3.4 Die Parteien verwenden bestehende Standards, wie beispielsweise das European Standard Set (ESS) oder das Interpol Standard Set of Loci (ISSOL).

4. Regeln der DNA-Anfrage und Rückmeldung

- 4.1 Die Anfrage eines automatisierten Abrufs oder Abgleichs gemäß Artikel 3 und 4 des Vertrags enthält ausschließlich die folgenden Informationen;
 - 4.1.1 den Parteiencode der anfragenden Partei;
 - 4.1.2 das Datum, den Zeitpunkt und die Referenznummer der Anfrage;
 - 4.1.3 die DNA-Profile und deren Kennung;
 - 4.1.4 den Typ des übermittelten DNA-Profiles (offene Spur oder DNA-Personenprofil).
- 4.2 Die Parteien stellen sicher, dass die Anfragen voll mit den gemäß Artikel 2 Absatz 3 des Vertrags abgegebenen Erklärungen, wiedergegeben im Anhang A.3, übereinstimmen.
- 4.3 Die Rückmeldung (Vergleichsbericht) auf die Anfrage gemäß Punkt 4.1 wird an die nationale Kontaktstelle der anfragenden Partei übermittelt, damit festgestellt werden kann, ob ein Folgeersuchen zu stellen ist. Der Vergleichsbericht enthält ausschließlich folgende Informationen:
 - 4.3.1 die Angabe, ob eine oder mehrere Übereinstimmungen (Treffer) oder keine Übereinstimmung (kein Treffer) vorliegt;
 - 4.3.2 das Datum, den Zeitpunkt sowie die Referenznummer der Anfrage;
 - 4.3.3 das Datum, den Zeitpunkt und die Referenznummer der Rückmeldung;
 - 4.3.4 den Parteiencode der anfragenden Partei;
 - 4.3.5 die Kennung der anfragenden und der angefragten Partei;
 - 4.3.6 den Typ der übermittelten DNA-Profile (offene Spur oder DNA-Personenprofil);

4.3.7 im Fall des Abgleichs gemäß Artikel 4 des Vertrags das übereinstimmende DNA-Profil.

4.4 Die automatisierte Information über das Vorliegen eines Treffers erfolgt ausschließlich unter der Bedingung, dass der automatisierte Abruf oder Abgleich eine Übereinstimmung des im Anhang A.1 festgelegten Minimums an Loci ergeben hat. Im Fall eines Abrufs gemäß Artikel 3 des Vertrages ergreifen die nationalen Kontaktstellen der Parteien zu Zwecken der Verifikation geeignete Maßnahmen in Übereinstimmung mit ihrem innerstaatlichen Recht.

5. Kommunikationsnetzwerk für die Übermittlung der DNA-Daten

Der elektronische Austausch von DNA-bezogenen Daten zwischen den Parteien erfolgt unter Verwendung des "TESTA II" Kommunikationsnetzwerks gemäß den technischen Spezifikationen im Anhang A.5.

6. Maßnahmen zur Qualitätskontrolle

Die Parteien treffen die notwendigen Maßnahmen, um die Integrität der den anderen Parteien zur Verfügung gestellten oder zum Vergleich übermittelten DNA-Profile zu garantieren. Diese Maßnahmen müssen mit internationalen Standards übereinstimmen, wie zum Beispiel der ISO 17025. Die forensischen Aspekte dieser DNA-Profile müssen den im Anhang A.1. genannten Spezifikationen entsprechen.

Abschnitt 3: Daktyloskopische Daten

7. Übermittlung daktyloskopischer Daten

7.1 Zum Zweck der Umsetzung des Artikels 9 des Vertrags richten die Parteien einen gegenseitigen Zugang zu ihren "automatisierten Fingerabdruck- Identifizierungssystemen"(nachfolgend "AFIS" genannt) ein.

7.2 Die unter Punkt 7.1 genannten Systeme beinhalten ausschließlich automatisierte daktyloskopische Identifizierungssysteme, die zur Verhinderung und Verfolgung von Straftaten errichtet wurden. Administrative Daten dürfen nicht übermittelt werden.

7.3 Die Digitalisierung der daktyloskopischen Daten und ihre Übermittlung an die anderen Parteien erfolgt im Datenformat, das im "Interface Control Document (ICD)" im Anhang B.1 festgelegt ist. Jede Partei stellt sicher, dass die von den anderen Parteien übermittelten daktyloskopischen Daten mit den Fundstellendatensätzen in ihrem eigenen AFIS verglichen werden können.

7.4 Die in Artikel 9 des Vertrags genannten Fundstellendatensätze ermöglichen eine eindeutige Zuordnung zu einer Person oder Strafsache, sowie die Identifizierung der abrufenden Partei.

8. Abruf und Übermittlung der Ergebnisse

- 8.1 Die Parteien stellen sicher, dass die übermittelten daktyloskopischen Daten von ausreichender Qualität für einen AFIS-Vergleich sind. Die angefragte Partei prüft unverzüglich und vollautomatisiert die Qualität der übermittelten daktyloskopischen Daten. Sind die Daten für einen automatisierten Vergleich ungeeignet, informiert die angefragte Partei die anfragende Partei ohne Verzögerung.
- 8.2 Die angefragte Partei bearbeitet die Anfragen in der Reihenfolge, in der sie eingegangen sind. Die Anfragen müssen innerhalb von 24 Stunden vollautomatisiert bearbeitet werden. Die anfragende Partei kann, wenn das innerstaatliche Recht dies erfordert, die beschleunigte Bearbeitung dieser Anfrage erbitten. Die angefragte Partei bearbeitet diese Anfrage dann unverzüglich. Kann der Bitte aus Gründen, die die angefragte Partei nicht zu verantworten hat, nicht entsprochen werden, ist der Vergleich sofort nach Wegfall der Hindernisse durchzuführen.
- 8.3 Die angefragte Partei sorgt dafür, dass das System imstande ist, jeden "Treffer" bzw. "kein Treffer" voll automatisiert und ohne jede Verzögerung an die anfragende Partei zu übermitteln. Im Fall eines Treffers werden für alle übereinstimmenden daktyloskopischen Daten die in Artikel 9 Absatz 2 des Vertrags bezeichneten daktyloskopischen Daten und Kennungen gemäß den unter 10.1 festgelegten Kapazitäten übermittelt.

9. Kommunikationsnetzwerk für die Übermittlung daktyloskopischer Daten

Der elektronische Austausch daktyloskopisch-bezogener Daten zwischen den Parteien muss unter Verwendung des Kommunikationsnetzwerks "TESTA II" gemäß den technischen Spezifikationen im Anhang A.5 erfolgen.

10. Festlegung und Kapazitäten des automatisierten Abrufs daktyloskopischer Daten

- 10.1 Die maximale Anzahl der verschiedenen Typen der daktyloskopischen Daten (candidates), die pro Übermittlung zur Verifikation zugelassen werden, ist in Anhang B.2 festgelegt.
- 10.2 Die maximale Anfragekapazität pro Tag für daktyloskopische Daten von identifizierten Personen ist im Anhang B.3 für jede Partei festgelegt.
- 10.3 Die maximale Anfragekapazität pro Tag für daktyloskopische Spuren ist im Anhang B.4 für jede Partei festgelegt.

Abschnitt 4: Fahrzeugregisterdaten

11. Abrufverfahren und Übermittlung der Daten

- 11.1 Zum Zweck der Umsetzung des Artikels 12 des Vertrags richten die Parteien ein Netzwerk nationaler Kontaktstellen ein, um automatisierte Abrufe in ihren

Fahrzeugregisterdatenbanken durchzuführen. Die technischen Voraussetzungen des Datenaustauschs sind im Anhang C.3 festgelegt.

- 11.2 Unbeschadet der Bestimmungen des Vertrags und unter spezieller Berücksichtigung der Artikel 38 und 39 des Vertrags organisieren die Parteien sowohl als anfragende als auch als angefragte Partei die Verfahrensweise ihrer nationalen Kontaktstellen nach Treu und Glauben entsprechend den Bestimmungen und Grundsätzen des Vertrags.
- 11.3 Da sich die Parteien für ein voll automatisiertes Abrufverfahren entschieden haben, müssen sie sicherstellen, dass alle Anfragen ihre nach dem Vertrag vorgesehenen nationalen Kontaktstellen unter Aufsicht eines verantwortlichen Beamten passieren.

12. Kommunikationsnetzwerk für die Übermittlung von Fahrzeugregisterdaten

- 12.1 Die Parteien legen fest, für den elektronischen Austausch von Fahrzeugregisterdaten das Kommunikationsnetzwerk "TESTA II" und für das System gemäß Artikel 12 eine spezielle Version der EUCARIS Softwareanwendung zu verwenden, sowie jede modifizierte Version dieser beiden Systeme.
- 12.2 Alle Kosten, die aus der Verwaltung und der Verwendung des Systems gemäß Artikel 12 entstehen, einschließlich der Kosten für die EUCARIS-Technologie, müssen jährlich verhandelt und vereinbart werden.

13. Technische und organisatorische Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit

Die in Artikel 38 Absatz 2 des Vertrags angeführte technische Ausgestaltung des automatisierten Abrufverfahrens hinsichtlich Datenschutz, Datensicherheit, Vertraulichkeit und Unversehrtheit der Daten, Netzwerkverschlüsselungs- und Authentifizierungsverfahren sowie die Kontrolle der Zulässigkeit der Abrufe ist im Anhang C.2 geregelt.

Abschnitt 5: Polizeizusammenarbeit

14. Gemeinsame Einsatzformen

- 14.1 Durch einen Einsatzplan können zwei oder mehrere Parteien eine gemeinsame Einsatzform gemäß Artikel 24 des Vertrags bilden. Vor Beginn des Einsatzes treffen sie mündliche oder schriftliche Absprachen über die operativen Modalitäten des Einsatzes, wie zum Beispiel:
- a) die zuständigen Behörden der Parteien des Einsatzplans;
 - b) den spezifischen Zweck des Einsatzes;
 - c) den Gebietsstaat, in dem der Einsatz stattfindet;
 - d) den räumlichen Bereich des Gebietsstaats, in dem der Einsatz stattfindet;
 - e) den vom Einsatzplan umfassten Zeitraum;
 - f) die jeweilige vom Entsendestaat dem Gebietsstaat gewährte Unterstützung, einschließlich der Bereitstellung von Beamten oder anderen Behördenmitarbeitern, Material und finanziellen Mitteln;

- g) die am Einsatz teilnehmenden Beamten;
- h) den für den Einsatz verantwortlichen Beamten;
- i) die Befugnisse, die die Beamten und anderen Behördenmitarbeiter des Entsendestaates während des Einsatzes im Gebietsstaat ausüben dürfen;
- j) die jeweiligen Dienstwaffen, Ausrüstungsgegenstände und Munition, die die Beamten des Entsendestaats während des Einsatzes im Einklang mit den in Anhang D.3 genannten Regelungen verwenden dürfen;
- k) die logistischen Modalitäten bezüglich Transports, Unterbringung und Sicherheit;
- l) die Kostentragung für den gemeinsamen Einsatz, wenn diese von den Bestimmungen des Artikel 46 des Vertrags abweicht;
- m) sonstige erforderliche Elemente.

14.2 Eine Anfrage zur Bildung einer gemeinsamen Einsatzform kann durch die zuständige Behörde jeder Partei erfolgen. Im Anhang D.1 kann jede Partei die Behandlung eingehender Anfragen festlegen. Sofern kein Verfahren festgelegt ist, wird im Anhang D.1 eine nationale Kontaktstelle benannt, die den anderen Parteien hilft, ihre Anfragen an die zuständigen Behörden zu richten.

15. Grenzüberschreitende Einsätze bei gegenwärtiger Gefahr

- 15.1. Die Behörden, die gemäß Artikel 25 Absatz 3 des Vertrags unverzüglich zu unterrichten sind, sind im Anhang D.2 aufgelistet.
- 15.2 Jede Änderung der Kontaktdaten dieser Behörden wird so rasch wie möglich den ebenfalls im Anhang D.2 genannten Kontaktpunkten der anderen Parteien mitgeteilt.

16. Mitführen und Gebrauch von Dienstwaffen, Munition und Ausrüstungsgegenständen

Im Anhang D.3 listet jede Partei die Dienstwaffen, Munition und Ausrüstungsgegenstände auf, die gemäß Artikel 28 Absatz 1 Satz 3 des Vertrags nicht mitgeführt werden dürfen, die Dienstwaffen, Munition und Ausrüstungsgegenstände, die nicht gebraucht werden dürfen sowie die rechtlichen Bestimmungen gemäß Artikel 28 Absatz 2 des Vertrags und die praktischen Aspekte des Einsatzes von Dienstwaffen, Munition und Ausrüstungsgegenstände gemäß Artikel 28 Absatz 5 des Vertrags.

Abschnitt 6: Allgemeine Bestimmungen

17. Evaluierung der Anwendung und Umsetzung des Vertrags und der Durchführungsvereinbarung

- 17.1 Die Evaluierung der verwaltungsmäßigen und technischen Anwendung und Umsetzung des Vertrags und der Durchführungsvereinbarung wird von der gemeinsamen Arbeitsgruppe gemäß Artikel 43 Absatz 2 des Vertrags oder von einer technischen Arbeitsgruppe, die zu diesem Zweck von der gemeinsamen Arbeitsgruppe beauftragt wurde, durchgeführt. Eine solche Evaluierung erfolgt auf Antrag einer Partei.

17.2 Die Modalitäten des automatisierten Abrufs und Abgleichs von DNA-Daten beziehungsweise daktyloskopischen Daten werden, sofern die gemeinsame Arbeitsgruppe nichts anderes beschließt, sechs Monate nach Aufnahme der Tätigkeiten auf Grundlage dieser Durchführungsvereinbarung evaluiert. In Bezug auf die Fahrzeugregisterdaten erfolgt die erste Evaluierung drei Monate nach Aufnahme der Tätigkeiten. Danach wird eine Evaluierung auf Antrag einer Partei gemäß Artikel 43 des Vertrags durchgeführt.

17.3 Die gemäß Artikel 39 Absatz 2 des Vertrags für die Protokollierung zuständigen Stellen haben Stichproben in einer solchen Häufigkeit und im notwendigen Umfang vorzunehmen, um eine effektive Kontrolle der Rechtmäßigkeit der automatisierten Abrufe gemäß der Artikel 3, 9 und 12 des Vertrags durch die nationalen Kontaktstellen der anderen Parteien sicherzustellen.

18. Verfügbarkeit des automatisierten Datenaustauschs

Die Parteien treffen alle notwendigen Vorkehrungen, damit der automatisierte Online-Austausch von DNA-Daten, daktyloskopischen Daten und Fahrzeugregisterdaten rund um die Uhr und sieben Tage die Woche möglich ist. Im Fall einer technischen Störung informieren die nationalen Kontaktstellen der Parteien einander so rasch wie möglich und vereinbaren in der Zwischenzeit einen alternativen Informationsaustausch gemäß den geltenden rechtlichen Regelungen. Der automatisierte Datenaustausch ist so schnell wie möglich wieder herzustellen.

19. Änderungen der Durchführungsvereinbarung und ihrer Anhänge

19.1 Jede Partei kann Änderungen dieser Durchführungsvereinbarung und ihrer Anhänge vorschlagen. Diese Vorschläge werden allen anderen Parteien mitgeteilt.

19.2 Bezieht sich die vorgeschlagene Änderung auf die Bestimmungen der Durchführungsvereinbarung wird diese durch eine Entscheidung des Ministerkomitees gemäß Artikel 43 Absatz 1 des Vertrags getroffen.

19.3 Bezieht sich die vorgeschlagene Änderung auf einen oder mehrere der Anhänge der Durchführungsvereinbarung wird diese durch die gemeinsame Arbeitsgruppe gemäß Artikel 43 Absatz 2 des Vertrags angenommen.


19.4 Für die Änderung dieser Durchführungsvereinbarung oder ihrer Anhänge ist Einstimmigkeit gegeben, wenn die anwesenden und vertretenen Parteien einer vorgeschlagenen Änderung zustimmen. Folglich wird die Annahme einer Änderung der Durchführungsvereinbarung durch die abwesenden und nicht vertretenen Parteien nicht verhindert. Eine angenommene Änderung ist für alle Parteien wirksam.

20. Wirksamkeit; Unterzeichnung; Verwahrung

- 20.1 Für jene Parteien, für die der Vertrag bereits in Kraft getreten ist, wird die Durchführungsvereinbarung nach der Unterzeichnung und der Annahme der erforderlichen Beschlüsse gemäß Artikel 34 Absatz 2 des Vertrags wirksam. Für andere Parteien wird sie gemäß Artikel 50 Absatz 1 beziehungsweise Artikel 51 Absatz 1 des Vertrags sowie nach Annahme der erforderlichen Beschlüsse gemäß Artikel 34 Absatz 2 des Vertrags wirksam.
- 20.2 Die Durchführungsvereinbarung und ihre Anhänge werden in deutscher, spanischer, französischer, niederländischer und englischer Sprache unterzeichnet, wobei jeder Wortlaut gleichermaßen verbindlich ist.
- 20.3 Die Regierung der Bundesrepublik Deutschland ist Verwahrer dieser Durchführungsvereinbarung und ihrer Anhänge.

Brüssel, der 5. Dezember 2006

Für das Königreich Belgien

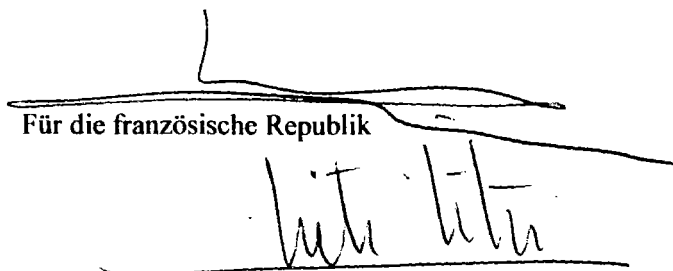


Für die Bundesrepublik Deutschland

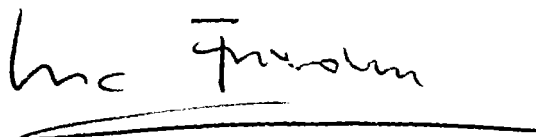


Für das Königreich Spanien

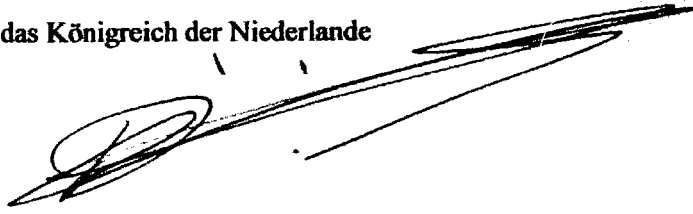
Für die französische Republik



Für das Großherzogtum Luxemburg



Für das Königreich der Niederlande

A handwritten signature in black ink, appearing to be a stylized 'D' followed by several horizontal strokes, positioned below the text 'Für das Königreich der Niederlande'.

Für die Republik Österreich

Stim Prokuf ad. oct.

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. For 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_ty	Type of profile

	pe	
result	PRUEM_datas_res ult	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_profil e	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_hitqualit y_type	Quality of Hit
HITCOUNT	Integer	Count of matched Alleles

2.3.2. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: <ol style="list-style-type: none"> 1. Case "No Hit": original requesting profile sent back only; 2. 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

2.3.3. PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

2.3.4. 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

2.3.5. IPSPG_DNA_profile

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

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

2.3.6. IPSPG_DNA_ISSOL

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

Fields	Type	Description
Vwa	IPSPG_DNA_locus	Locus vwa
th01	IPSPG_DNA_locus	Locus th01
D21s11	IPSPG_DNA_locus	Locus d21s11

Fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
Amelogenin	IPSG_DNA_locus	Locus amelogenin

2.3.7. 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

2.3.8. 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 (Trans European Services for Telematics between Administrations) 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.

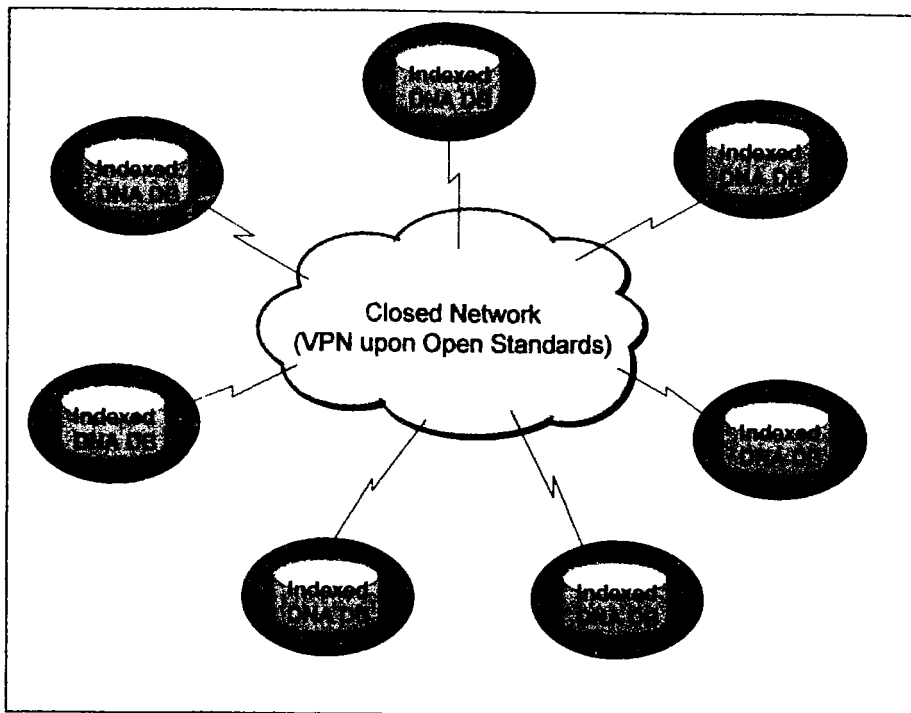
Each Party will decide which option to take by itself. This access scheme should be accepted by future acceding States to the Treaty.

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.

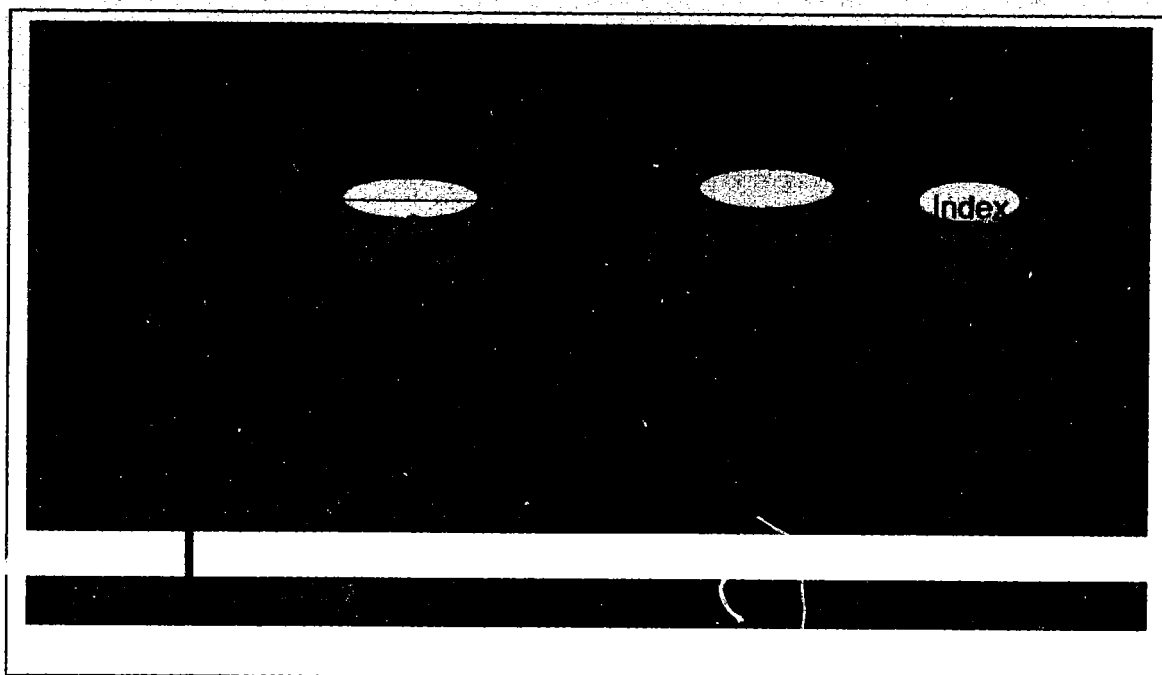
Because of sMIME's easy integration into national IT infrastructure at all Parties' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal "Proof of Concept" in a more efficient way and reducing costs the open standard JavaMail API is however 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 (Java Cryptographic Extension) 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 eXtensible Markup Language (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

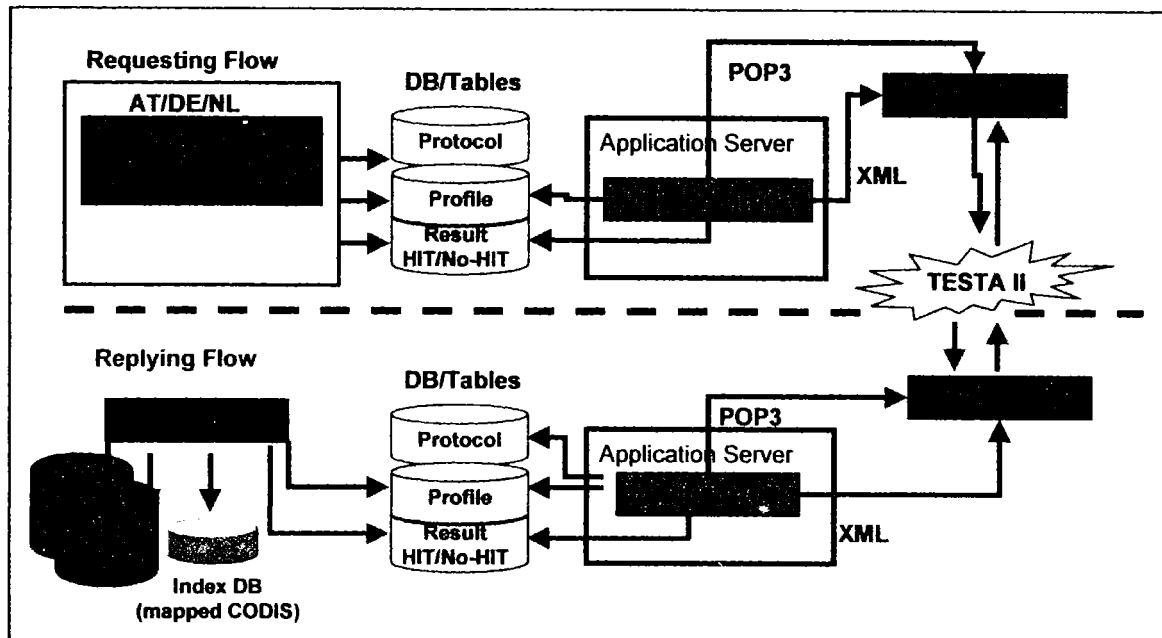
Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has however certain drawbacks. Administering a large number of client machines can involve a diversity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

6.3 JDBC

Java DataBase Connectivity (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



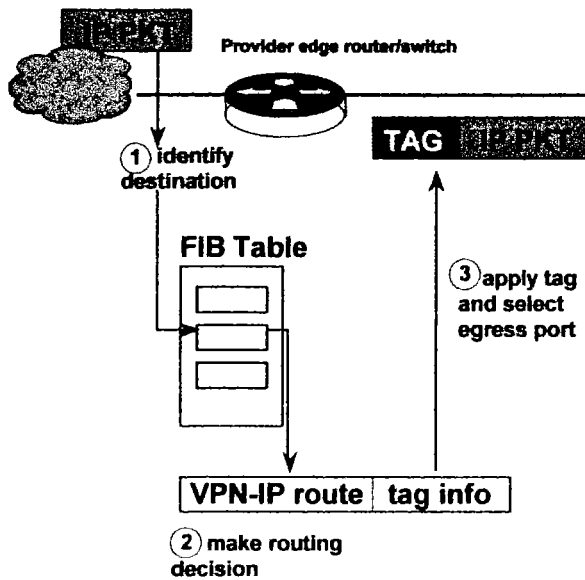
7. Communication Environment

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 Domain Name Services (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 Mail Transfer Protocol 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 **Post Office Protocol 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
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	<i>dna.pruem.at.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.at.eu-admin.net</i>	
Belgium	<i>dna.pruem.be.eu-admin.net</i>	Setting up a secure local link to the existing TESTA II access point
	<i>fp.pruem.be.eu-admin.net</i>	
Germany	<i>dna.pruem.de.eu-admin.net</i>	Using the existing TESTA II national access points
	<i>fp.pruem.de.eu-admin.net</i>	
Spain	<i>dna.pruem.es.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.es.eu-admin.net</i>	
France	<i>dna.pruem.fr.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.fr.eu-admin.net</i>	
Luxemburg	<i>dna.pruem.lu.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.lu.eu-admin.net</i>	
The Netherlands	<i>dna.pruem.nl.eu-admin.net</i>	Intending to establish a new TESTA II access point at the NFI
	<i>fp.pruem.nl.eu-admin.net</i>	

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 minutiae 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 minutiae 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 minutiae 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	1	2	3	4	5	6
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 MEAN TIME (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 represent 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 field 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 field 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 field contains the SQN (field 2.008) transmitted by an MPS or MMS transaction.

4.1.11 FIELD 2.015: MISCELLANEOUS IDENTIFICATION NUMBER (MN4)

This field 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

Numeric Code (1-3)	Meaning (5-128)
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 than 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
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: MINUTIAE RECORD

Type-9 records shall contain ASCII text describing minutiae 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 MINUTIAE 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.

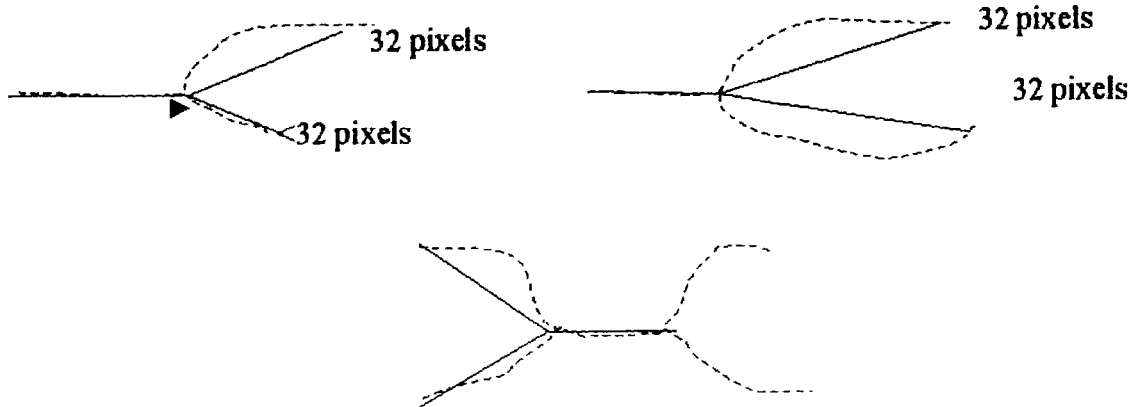
The position or location of a minutia representing a ridge ending shall be the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the three legs of the valley area were thinned down to a single-pixel-wide skeleton, the point of the intersection is 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 MINUTIAE 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 minutiae 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: MINUTIAE 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 minutiae 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 minutiae record.

6.2.15 FIELD 9.136: NUMBER OF MINUTIAE

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

6.2.16 FIELD 9.137: FINGER MINUTIAE 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	Con d. code	Field Numbe r	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
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	--	--	--	--	--	--

Ident	Con- d. code	Field Numbe r	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
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	Con d. cod e	Field Numb er	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	Con d. cod e	Field Numb er	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 (mm²)	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.

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

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.

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
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 2{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}99999 9{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	A	2.015:A{GS}

			Identification Number		
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 ¹	Remarks	Prüm Y/N ²
Data relating to vehicles			
Licence number	M		Y
Chassis number / VIN	M		Y
Party of registration	M		Y
Make	M	(D.1 ³) e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
Nature of the vehicle / EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y

2.2.2 Complete data set

Item	M/O ⁴	Remarks	Prüm Y/N
Data relating to holders of the vehicle			
(C.1⁵)			
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,	Y

¹ M = mandatory when available in national register, O = optional

² All the attributes specifically allocated by the Parties are indicated with Y.

³ Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

⁴ M = mandatory when available in national register, O = optional

⁵ Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

Item	M/O ⁴	Remarks	Prüm Y/N
		Zip code, Place of residence, Party of residence etc., and the Address in printable format will be communicated	
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
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

Item	M/O ⁴	Remarks	Prüm Y/N
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 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.

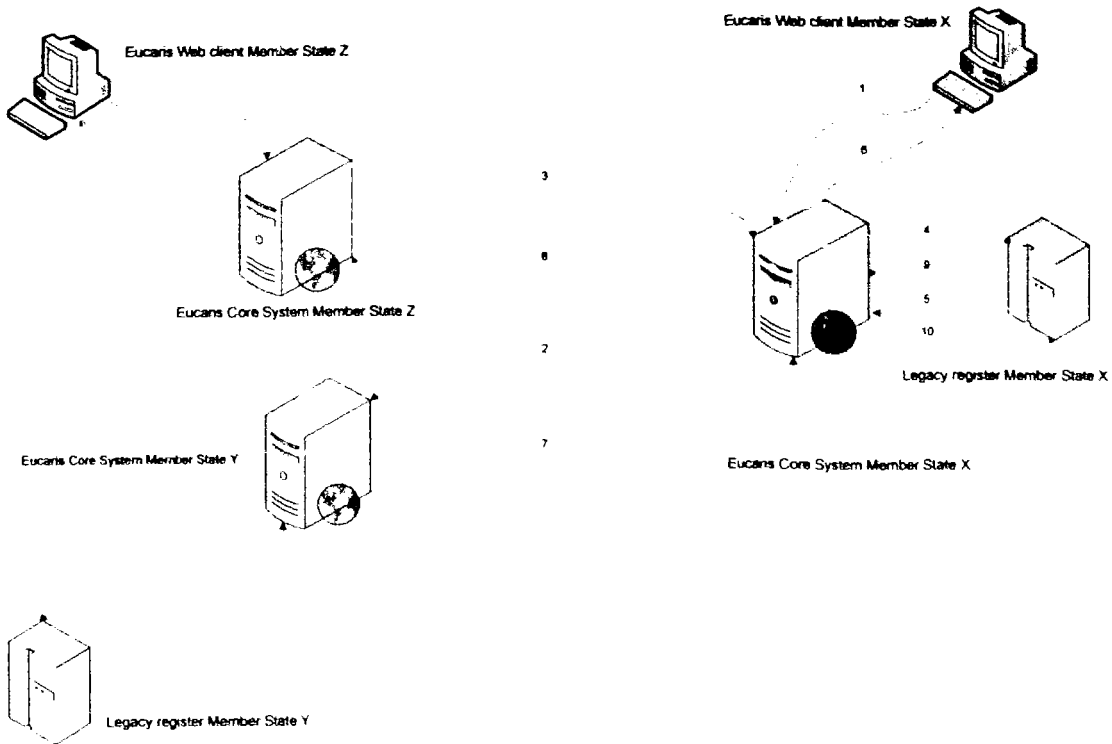


Figure : Message types for logging

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.

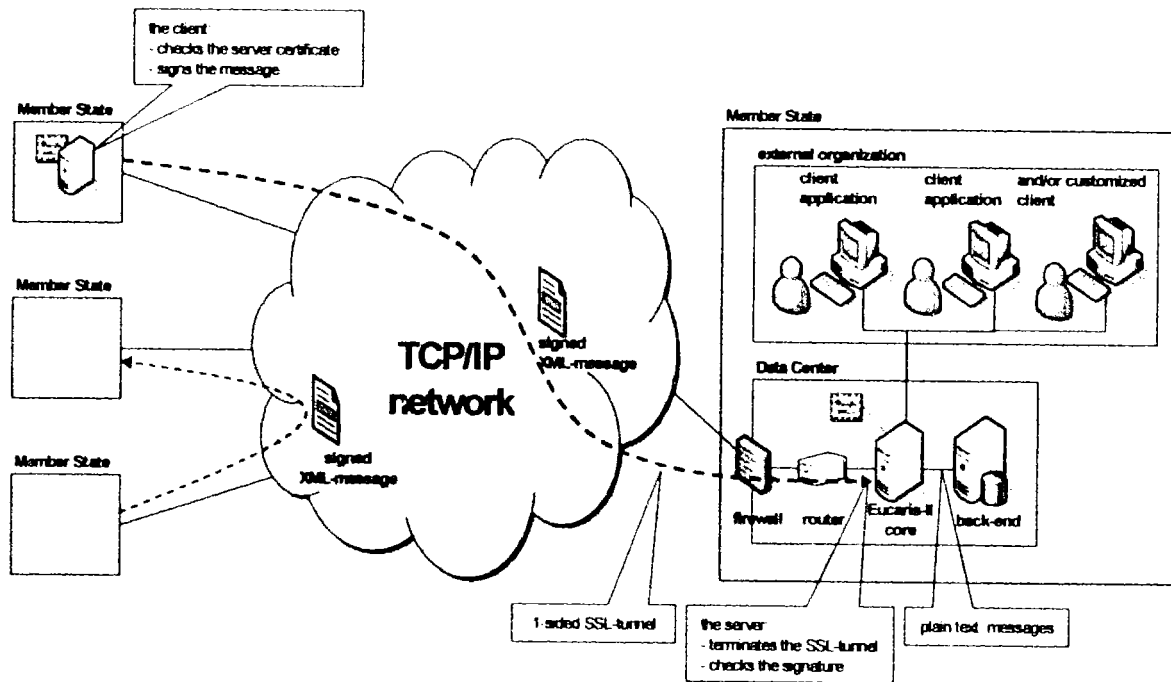
Annex C.3

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/O⁶	Remark
Network concept	M	The concept is an “any-to-any” communication.
Physical network	M	TESTA
Core application	M	<p>The core application of EUCARIS has to be used to connect to the other Parties. The following functionality is offered by the core:</p> <ul style="list-style-type: none"> ▪ 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.
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 acceptance 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.

⁶ M = mandatory to use or to comply with O = optional to use or to comply with

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.

Nr.	Description
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.
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

Nr.	Description
	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.
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

Nr.	Description
	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.

Nr.	Description
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

Nr.	Description
	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	<u>Help.div@mobiliteit.fgov.be</u> (DIV) <u>Help.ict@mobiliteit.fgov.be</u> (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	+34915371883	+34913191228	

	de Seguridad (Ministry of Interior)	+34915371884 +34915372056 +34915372057 +34915372058	+34913191645 +34913197389	ceplic@ses.m ir.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@l.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)

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@l.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 : 04 68 83 79 10 Tel : 05 59 20 93 60 Fax : 05 59 20 59 34 E-mail : ccpd-hendaye@interieur.gouv.fr ccpd-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 Article 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 Kontaktstelle, 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 Polizeianglegenheiten;
Terrorismusbekämpfung

Tel.: +49 (0) 1888 681-1077

Fax.: +49 (0) 1888 681-2926

Mail: poststelle@bmi.bund.de

- für die Bundespolizei:
Abteilung für Angelegenheiten der
Bundespolizei

Tel.: +49 (0) 1888 681-0

Fax: +49 (0) 1888 681-1829

Mail: poststelle@bmi.bund.de

Alt-Moabit 101D
D-10559 Berlin

Co-operation where consent must be obtained from a Land interior ministry. In the following you will find the Bundesländer, 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: lageszentrum@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 Wiesbaden

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: lageszentrum@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

Tel.: +49 351 564 3775 oder 3776

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

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 or 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

Competent authorities: Police and Royal Constabulary (Koninglijke Marechaussee)

Memberstates	Organisation	Central point of contact	Telephone number Fax number E-mail
AUSTRIA BELGIUM GERMANY FRANCE LUXEMBURG	Korps Landelijke Politie Diensten (KLPD) Department for Conflict and	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	Crisismanagement Koninklijke Marechaussee (Royal Constabulary) Commander of National and Foreign Squads	Kamp Nieuw Millingen Postbus 59 3886 ZH Garderen	Tel: (0031)(0)577455766 Fax:(0031)(0)577455763
-------	---	--	---

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:

Gabinete 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	Landespolizeikommand o Oberösterreich - Landesleitzentrale		Tel.: +43 (0) 59133 40-2222 Fax: +43 (0) 59133 40-1009 Mail: <u>LPK-</u> <u>O@polizei.gv.at</u>
	Landespolizeikommand o Salzburg - Landesleitzentrale		Tel.: +43 (0) 59133 50-2222 Fax: +43 (0) 59133 50-1009 Mail: <u>LPK-</u> <u>S@polizei.gv.at</u>
	Landespolizeikommand o Tirol - Landesleitzentrale		Tel.: +43 (0) 59133 70-2222 Fax: +43 (0) 59133 70-1009 Mail: <u>LPK-</u> <u>T@polizei.gv.at</u>
	Landespolizeikommand o Vorarlberg - Landesleitzentrale		Tel.: +43 (0) 59133- 80-2222 Fax: +43 (0) 59133- 80-1009 Mail: <u>LPK-</u> <u>V@polizei.gv.at</u>
OTHER PARTYS	Federal Ministry of the Interior, Division II – General Directorate for Public		Phone: +431-53126- 3200 or -3775 Fax: +431-53126-3120 e-mail: <u>bmi-II-EKC-</u>

	Security, Operations and Crisis Coordination Centre		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/LANGEMARK-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
	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/	+ 32 (0) 80 28.14.10

		BURG-REULAND/ SANKT-VITH	
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/VIELSAL M	+32 (0)84 31.03.11
	PZ 5291 EIFEL	AMEL /BULLINGEN/ BUTGENBACH/ BURG-REULAND/ SANKT-VITH	+ 32 (0) 80 28.14.10
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	EKLO / 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
	PZ 5382	VOEREN	+ 32 (0)4 381.10.11
	PZ 5288 PAYS DE HERVE	AUBEL/BAELEN/HERVE/LIMBOU RG/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@l.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)
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.fr cpd-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	Local contactpoints of the police (Police of the Länder	All municipalities at the borders with the Prüm	

(AT, FR, LU, BE, NL)	and Bundespolizei)	partners	
	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		

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
-------------	--------------	-----------------	--------------------------------

<p>BELGIUM GERMANY</p>	<p>Korps Landelijke Politiediensten (KLPD) (Police) Bureau Conflict-en Crisisbeheersing</p> <p>Or:</p> <p>Local contactpoints of the regional policeforces</p> <p>In the event of a border crossing, the competent regional Police Communications Centre (Gemeenschappelijk meldkamer) must be informed immediately</p>	<p>Hoofdstraat 54 Postbus 100 3970 AC Driebergen</p>	<p>E-mail Tel: (0031)(0)343536366 Fax:(0031)(0)343518180 E- mail:ccb.klpd@klpd.politi e.nl</p>
-----------------------------------	---	--	---

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

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

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: <u>ss-ccpa-</u> <u>hendaya@guardiacivil.org</u> Timetable: 24 hours a day
	CCPD	SOMPORT (Huesca)	Tel: 00 34 974 373572 Fax:00 34 974 373573 E-mail: <u>hu-cmd-huesca-</u> <u>ccpasomport@guardiacivi</u> <u>l.org</u> 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: <u>l-ccpa-</u> <u>melles@guardiacivil.org</u> Timetable: Monday – Friday 08:00 - 21:00 Saturday – Sunday 09:00 - 17:00

PROVINCE HEAD QUARTERS	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

REGION	UNIT	ADRESS	TELEFONO	FAX
Pais Vasco	Headquarters of San Sebastián	C/ José M 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
Cataluna	Headquarters of Girona	C/ Sant Pau, 2	34.972.220025	34.972.201149
Cataluna	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:

+ 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:

ceplic@ses.mir.es

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:

1. 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.
2. 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 recent 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 robbery 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 be 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 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. 1^{er}. 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 1^{er}:

- 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 immobiliser 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 1^{er} opérant d'office ou sur les ordres de leurs supérieurs hiérarchiques ou sur la réquisition de l'autorité judiciaire peuvent immobiliser 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 Tötlichkeiten 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 entflozene 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, Sperrn, 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 special 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 rifle, 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 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 deprivation 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 ammunition 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 grenades 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 of his 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 deportation 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 unconscious 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 surveillance

Article 31

1. After receiving the consent of the assistant district attorney, the officer can subject the detainee to permanent video surveillance.
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 surveillance and shall make a record of the permanent video surveillance.

§ 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 published 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.

Acuerdo de Ejecución

del Tratado entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, firmado en Prüm, Alemania, el 27 de mayo de 2005

Sección 1: Objeto y definiciones

1 Objeto

De conformidad con el artículo 44 del Tratado, el objeto del presente Acuerdo de Ejecución es adoptar las disposiciones necesarias para la ejecución y aplicación administrativa y técnica del Tratado.

2 Definiciones

A los efectos del presente Acuerdo de Ejecución:

- 2.1 por "Tratado" se entenderá el Tratado entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria, relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, firmado en Prüm, Alemania, el 27 de mayo de 2005;
- 2.2 por "Parte" se entenderá toda Parte Contratante del Tratado que haya firmado el presente Acuerdo de Ejecución;
- 2.3 por los procedimientos de "consulta", "comparación" y "consulta mediante comparación" a que se refieren los artículos 3, 4 y 9 del Tratado se entenderá los procedimientos por los que se determine si existe una concordancia entre los datos de ADN o datos dactiloscópicos que hayan sido comunicados por una Parte y los datos de ADN o datos dactiloscópicos almacenados en las bases de datos de una, varias o todas las demás Partes;
- 2.4 por "perfil de ADN" se entenderá un código alfabético o numérico que represente un conjunto de características identificativas de la parte no codificante de una muestra de ADN humano analizada, es decir, la forma química concreta en las distintas ubicaciones del ADN (loci);
- 2.5 por "parte no codificante del ADN" se entenderá las zonas cromosómicas que no contienen ninguna expresión genética, es decir, de las que no se sabe que proporcionen información sobre características hereditarias específicas;
- 2.6 por "datos de referencia del ADN" se entenderá un perfil de ADN y los datos conexos no específicos del ADN;
- 2.7 por "datos no específicos del ADN" se entenderá:
 - 2.7.1 un código o número de identificación que permita a las Partes, en caso de concordancia, recuperar los datos de carácter personal u otra información disponible en sus bases de datos para transmitirla a una, varias o todas las Partes en virtud de lo dispuesto en el artículo 5 del Tratado,

- 2.7.2 un código de Parte que indique el origen nacional del perfil de ADN; y
- 2.7.3 un código indicativo del tipo de perfil de ADN según lo declarado por las Partes con arreglo al artículo 2, apartado 2, del Tratado;
- 2.8 por “perfil de ADN no identificado” se entenderá el perfil de ADN obtenido a partir de vestigios procedentes de la investigación de delitos y pertenecientes a personas todavía no identificadas;
- 2.9 la expresión “perfil de ADN de referencia” es de carácter técnico y por la misma se entenderá el perfil de ADN de una persona identificada incluido en los ficheros nacionales de análisis del ADN mencionados en el artículo 2, apartado 3, del Tratado;
- 2.10 por “datos dactiloscópicos” se entenderá las imágenes de huellas dactilares, imágenes de huellas dactilares latentes, huellas palmares, huellas palmares latentes y los patrones de dichas imágenes (minucias) que estén almacenados y organizados en una base de datos automatizada;
- 2.11 por “solicitud de seguimiento” se entenderá la solicitud enviada por una Parte a una, varias o todas las demás Partes en caso de concordancia de los datos de ADN o dactiloscópicos comparados, con el fin de obtener otros datos de carácter personal e información de otro tipo con arreglo a los artículos 5 y 10 del Tratado;
- 2.12 por “datos procedentes de los registros de matriculación de los vehículos” se entenderá los conjuntos de datos indicados en el Anexo C.1 que las Partes hayan acordado poner a disposición mutua para un procedimiento de consulta automatizada en el sentido del siguiente punto 2.13;
- 2.13 por “consulta automatizada” se entenderá un procedimiento de acceso en línea para consultar, con arreglo a lo dispuesto en el artículo 33, apartado 1, punto 2, del Tratado, las bases de datos de una, varias o todas las demás Partes;
- 2.14 por “el sistema previsto en el artículo 12” se entenderá el conjunto de medidas técnicas y aspectos funcionales, como las cuestiones relacionadas con redes, interfaces y seguridad, adoptados para el intercambio de datos procedentes de los registros de matriculación de vehículos con arreglo al artículo 12 del Tratado;
- 2.15 Por “EUCARIS” se entenderá el Sistema europeo de información sobre vehículos y permisos de conducción creado por el correspondiente Tratado, firmado en Luxemburgo el 29 de junio de 2000;
- 2.16 por “casos concretos”, en el sentido del artículo 3, apartado 1, artículo 9, apartado 1, y artículo 12, apartado 1, del Tratado, se entenderá un mismo expediente de investigación o expediente de actuación penal; si dicho expediente contiene más de un perfil de ADN, dato dactiloscópico o dato de matriculación de vehículo, todos ellos podrán transmitirse juntos como una única consulta;

- 2.17 por "motivo de la consulta o de la transmisión de datos" se entenderá, a efectos de la aplicación del artículo 39 del Tratado, una indicación que permita establecer un vínculo claro entre una solicitud determinada y el caso concreto correspondiente que dio lugar a la solicitud;
- 2.18 por "red de comunicación TESTA II" se entenderá los "Servicios transeuropeos de telemática entre administraciones" gestionados por la Comisión Europea, así como cualquier versión modificada de los mismos.

Sección 2: Perfiles de ADN

3 Composición y comparación de perfiles de ADN

- 3.1 A efectos de la aplicación del artículo 2 del Tratado, los datos de referencia del ADN que se intercambiarán en virtud de lo dispuesto en el Tratado estarán compuestos por un perfil de ADN y por los datos no específicos del ADN.
- 3.2 Se elaborarán una serie de especificaciones técnicas comunes, que incluirán reglas de concordancia, algoritmos y códigos numéricos de las Partes, según lo establecido en los Anexos A, y se distribuirán a todos los puntos de contacto nacionales de las Partes para su aplicación a todas las solicitudes y respuestas relacionadas con la consulta o la comparación de perfiles de ADN, con arreglo a lo dispuesto en el punto 3.1.
- 3.3 Los perfiles de ADN se compararán sobre la base de marcadores compartidos según se dispone en el Anexo A.1. Todo perfil de ADN transmitido para la consulta o la comparación automatizadas por la Parte requirente se comparará con todos los perfiles de ADN que las Partes requeridas hayan hecho accesibles para la comparación con arreglo al artículo 2, apartados 2 y 3, del Tratado.
- 3.4 Las Partes harán uso de las normas existentes, como el Conjunto Normalizado de Loci para Europa (ESS) o el Conjunto Normalizado de Loci de INTERPOL (ISSOL).

4 Reglas aplicables a las solicitudes y respuestas en materia de ADN

- 4.1 La solicitud de consulta o de comparación automatizada con arreglo a los artículos 3 y 4 del Tratado incluirá exclusivamente la siguiente información:
- 4.1.1 el código de Parte de la Parte requirente;
 - 4.1.2 la fecha, hora y número de referencia de la solicitud;
 - 4.1.3 los perfiles de ADN y los correspondientes datos no específicos del ADN;
 - 4.1.4 el tipo de perfiles de ADN transmitidos (perfiles de ADN no identificados o perfiles de ADN de referencia)
- 4.2 Las Partes harán lo necesario para que las solicitudes se ajusten plenamente a las condiciones impuestas mediante las declaraciones mencionadas en el artículo 2,

apartado 3, del Tratado y que se reproducen en el Anexo A.3.

- 4.3 La respuesta (informe de concordancia) a la solicitud mencionada en el punto 4.1 se enviará al punto de contacto nacional de la Parte requirente para averiguar si es posible que se realice una solicitud de seguimiento. El informe de concordancia contendrá únicamente la siguiente información:
- 4.3.1 la indicación de si se han encontrado uno o varios perfiles coincidentes o ninguno;
 - 4.3.2 la fecha, hora y número de referencia de la solicitud;
 - 4.3.3 la fecha, hora y número de referencia de la respuesta;
 - 4.3.4 el código de Parte de la Parte requerida;
 - 4.3.5 los datos no específicos del ADN de la Parte requirente y de la Parte requerida;
 - 4.3.6 el tipo de perfiles de ADN transmitidos (perfiles de ADN no identificados o perfiles de ADN de referencia);
 - 4.3.7 en caso de comparación con arreglo al artículo 4 del Tratado, el perfil de ADN concordante.
- 4.4 Únicamente se notificará automáticamente una concordancia cuando la consulta o comparación automatizada haya dado como resultado la coincidencia de un número mínimo de loci con arreglo a lo dispuesto en el Anexo A.1. En caso de consulta en virtud del artículo 3 del Tratado, a efectos de verificación, los puntos de contacto nacionales de las Partes tomarán las medidas adecuadas de conformidad con su derecho interno.

5 Red de comunicación para la transmisión de datos del ADN

El intercambio electrónico de datos relacionados con el ADN entre las Partes se efectuará a través de la red de comunicación TESTA II, con arreglo a las especificaciones técnicas indicadas en el Anexo A.5.

6 Medidas de control de la calidad

Las Partes tomarán las medidas adecuadas para garantizar la integridad de los perfiles de ADN puestos a disposición de las demás Partes o transmitidos para su comparación. Estas medidas se ajustarán a las normas internacionales, como ISO 17025. Los aspectos forenses de estos perfiles de ADN deberán ajustarse a las especificaciones expresadas en el Anexo A.1.

Sección 3: Datos dactiloscópicos

7 Transmisión de datos dactiloscópicos

- 7.1 A efectos de la aplicación del artículo 9 del Tratado, las Partes establecerán un sistema de acceso técnico recíproco a sus "sistemas automatizados nacionales de identificación dactiloscópica" (en adelante denominados AFIS).

- 7.2 Los sistemas mencionados en el punto 7.1 serán únicamente los sistemas automatizados de identificación dactiloscópica creados para la prevención y la investigación de los delitos. No podrán transmitirse los datos contenidos en expedientes administrativos.
- 7.3 La digitalización de los datos dactiloscópicos y su transmisión a otras Partes se efectuará con arreglo al formato de datos especificado en el "Documento de Control de Interfaces" (ICD) definido en el Anexo B.1. Cada Parte se asegurará de que los datos dactiloscópicos transmitidos por las demás Partes puedan compararse con los datos de referencia de su propio AFIS.
- 7.4 Las referencias mencionadas en el artículo 9 del Tratado permitirán establecer la correspondencia unívoca con una persona o un asunto penal, así como la identificación de la Parte requirente.

8 Consulta y transmisión de resultados

- 8.1 Las Partes se asegurarán de que los datos dactiloscópicos transmitidos sean de una calidad adecuada para su comparación por AFIS. La Parte requerida comprobará inmediatamente, por un procedimiento plenamente automatizado, la calidad de los datos dactiloscópicos transmitidos. En caso de que los datos no sean adecuados para una comparación automatizada, la Parte requerida informará sin demora a la Parte requirente.
- 8.2 La Parte requerida efectuará las consultas en el orden en que se reciban las solicitudes. Las solicitudes deberán tramitarse en el plazo de 24 horas por un procedimiento plenamente automatizado. La Parte requirente podrá pedir, cuando así lo exija su derecho interno, una tramitación urgente de estas consultas. La Parte requerida llevará a cabo esas consultas inmediatamente. Si no pueden cumplirse estos plazos por causas no imputables a la Parte requerida, la comparación deberá efectuarse lo antes posible una vez desaparecidos los impedimentos.
- 8.3 La Parte requerida velará por que el sistema esté en condiciones de transmitir inmediatamente a la Parte requirente, de forma plenamente automatizada, la existencia o no de concordancias. En caso de concordancia, transmitirá los datos dactiloscópicos y las referencias indicadas en el artículo 9, apartado 2, del Tratado respecto de todas las concordancias entre datos dactiloscópicos.

9 Red de comunicación para la transmisión de datos dactiloscópicos

El intercambio electrónico de datos dactiloscópicos y datos relacionados con los mismos entre las Partes se efectuará a través de la red de comunicación TESTA II, con arreglo a las especificaciones técnicas indicadas en el Anexo A.5.

10 Definición y capacidades de la consulta automatizada de datos dactiloscópicos

- 10.1 En el Anexo B.2 se indica el volumen máximo de los distintos tipos de datos dactiloscópicos ("candidatos") que se aceptará para su verificación por cada transmisión.
- 10.2 En el Anexo B.3 se indica, respecto de cada Parte, su capacidad máxima diaria de investigación de datos dactiloscópicos de personas identificadas.
- 10.3 En el Anexo B.4 se indica, respecto de cada Parte, su capacidad máxima diaria de investigación de rastros dactiloscópicos.

Sección 4: Datos procedentes de los registros de matriculación de vehículos

11 Procedimiento de consulta y transmisión de resultados

- 11.1 A los efectos del artículo 12 del Tratado, las Partes establecerán una red de puntos de contacto nacionales para la realización de consultas automatizadas en sus respectivas bases de datos de matriculación de vehículos. En el Anexo C.3 se recogen las condiciones técnicas para el intercambio de datos.
- 11.2 Sin perjuicio de las disposiciones del Tratado, y tomando especialmente en consideración sus artículos 38 y 39, las Partes, ya intervengan como Parte requirente o requerida, organizarán el funcionamiento de sus puntos de contacto nacionales, con el debido respeto a las disposiciones y los principios del Tratado.
- 11.3 Las Partes que opten por un procedimiento de consulta totalmente automatizado deberán garantizar que todas sus solicitudes se canalicen a través de su punto de contacto nacional previsto en el Tratado, que estará sometido a la supervisión de un funcionario responsable.

12 Red de comunicación para la transmisión de datos procedentes de los registros de matriculación de vehículos

- 12.1 Para el intercambio electrónico de datos procedentes de los registros de matriculación de vehículos, las Partes deciden utilizar la red de comunicación TESTA II y una aplicación de software de EUCARIS especialmente diseñada para los fines del sistema previsto en el artículo 12, así como cualquier versión modificada de ambos sistemas.
- 12.2 Se estudiarán y acordarán anualmente todos los costes derivados de la gestión y utilización del sistema previsto en el artículo 12 que deban ser objeto de reparto, incluidos los relacionados con la tecnología EUCARIS.

13 Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad

En el Anexo C.2 se detallan las especificaciones técnicas para la consulta automatizada, con arreglo a lo dispuesto en el artículo 38, apartado 2, del Tratado, en lo que respecta a la protección, seguridad, confidencialidad e integridad de los datos, el cifrado en red y los procedimientos de autorización, así como los procedimientos de control de la admisibilidad de las consultas automatizadas.

Sección 5: Cooperación policial

14 Intervenciones conjuntas

14.1 Mediante una declaración de misión, dos o más Partes podrán organizar una intervención conjunta con arreglo al artículo 24 del Tratado. Antes del inicio de la misma, acordarán por escrito o de palabra todo lo relativo a la forma de la intervención, a saber:

- a) las autoridades competentes de las Partes en la declaración de misión;
- b) la finalidad concreta de la intervención;
- c) el Estado del territorio en que se desarrollará la intervención;
- d) la zona geográfica del Estado del territorio en que se desarrollará la intervención;
- e) el periodo de tiempo a que se refiere la declaración de misión de la intervención;
- f) la ayuda concreta que debe proporcionar al Estado del territorio el Estado de origen, que comprenderá agentes u otros funcionarios, material y fondos;
- g) los agentes que participarán en la intervención;
- h) el agente que estará a cargo de la intervención;
- i) las facultades que podrán ejercer los agentes y otros funcionarios del Estado de origen en el Estado del territorio durante la intervención;
- j) las armas, municiones y equipos concretos que podrán utilizar los agentes enviados durante la intervención de conformidad con las reglas establecidas en el Anexo D.3;
- k) las cuestiones logísticas relacionadas con el transporte, el alojamiento y la seguridad;
- l) el reparto de los gastos de la intervención conjunta, cuando se aparte de lo dispuesto en el artículo 46 del Tratado;
- m) cualesquiera otros elementos necesarios.

14.2 La organización de una intervención conjunta podrá ser solicitada por las autoridades competentes de cualquiera de las Partes. En el Anexo D.1 se recogen los procedimientos establecidos por cada Parte para el envío de solicitudes a la misma. Cuando no se establezca un procedimiento específico, el punto de contacto nacional indicado con arreglo al Anexo D.1 prestará asistencia a las demás Partes para dirigir sus solicitudes a las autoridades competentes.

15 Intervenciones con paso de frontera en caso de peligro inminente

- 15.1 En el Anexo D.2 figuran las autoridades a las que se deberá informar inmediatamente de conformidad con el artículo 25, apartado 3, del Tratado.
- 15.2 Cualquier modificación de los datos de contacto de esas autoridades se comunicará lo antes posible a los puntos de contacto de las demás Partes que se enumeran también en el Anexo D.2.

16 Empleo de armas de servicio, municiones y equipos

En el Anexo D.3 figura una enumeración, para cada Parte, de las armas de servicio, municiones y equipos concretos que se prohíbe llevar con arreglo al artículo 28, apartado 1, tercera frase, del Tratado, las armas de servicio, municiones y equipos concretos que se prohíbe utilizar y los correspondientes aspectos legales con arreglo al artículo 28, apartado 2, del Tratado, así como los aspectos prácticos mencionados en el artículo 28, apartado 5, del Tratado.

Sección 6: Disposiciones generales

17 Evaluación de la aplicación y ejecución del Tratado y del Acuerdo de Ejecución

- 17.1 De la evaluación de la aplicación y la ejecución técnica y administrativa del Tratado y del Acuerdo de Ejecución se encargará el Grupo de Trabajo Conjunto, con arreglo al artículo 43, apartado 2, del Tratado, o cualquier grupo de trabajo técnico al que el Grupo de Trabajo Conjunto encomiende esta misión. Esta evaluación podrá llevarse a cabo a petición de cualquiera de las Partes.
- 17.2 Salvo que el Grupo de Trabajo Conjunto decida otra cosa, las modalidades de consulta y comparación automatizadas de perfiles de ADN y datos dactiloscópicos se evaluarán una vez transcurridos seis meses desde el comienzo de las actividades sobre la base del presente Acuerdo de Ejecución. En el caso de los datos procedentes de los registros de matriculación de vehículos, la primera evaluación tendrá lugar a los tres meses del comienzo de las actividades. A partir de ese momento, las evaluaciones podrán realizarse a instancias de cualquier Parte, con arreglo al artículo 43 del Tratado.
- 17.3 Los órganos responsables del registro con arreglo al artículo 39, apartado 2, del Tratado, llevarán a cabo controles por muestreo con la frecuencia y el alcance necesarios para garantizar una evaluación efectiva de la legalidad de las consultas automatizadas efectuadas en virtud de los artículos 3, 9 y 12 del Tratado por los respectivos puntos de contacto extranjeros.

18 Disponibilidad del sistema de intercambio automatizado de datos

- 18.1 Las Partes harán todos los esfuerzos razonables para asegurar que el sistema automatizado de intercambio en línea de perfiles de ADN, datos dactiloscópicos y datos sobre matriculación de vehículos esté accesible las 24 horas del día, 7 días a la semana. En caso de fallo técnico, los correspondientes puntos de contacto de las Partes se informarán mutuamente lo antes posible y adoptarán de común acuerdo y con carácter temporal un medio de comunicación alternativo, de conformidad con cualquier otro instrumento legal aplicable. El intercambio automatizado de datos se restablecerá lo antes posible.

19 Modificación del Acuerdo de Ejecución y de sus Anexos

- 19.1 Cualquier Parte podrá proponer modificaciones del presente Acuerdo de Ejecución y de sus Anexos. Esas propuestas se comunicarán a todas las demás Partes.
- 19.2 Si la modificación propuesta se refiere a las disposiciones del Acuerdo de Ejecución, deberá aprobarse mediante decisión del Comité de Ministros con arreglo al artículo 43, apartado 1, del Tratado.
- 19.3 Si la modificación propuesta se refiere a uno o varios Anexos del Acuerdo de Ejecución, será aprobada por el Grupo de Trabajo Conjunto previsto en el artículo 43, apartado 2, del Tratado.
- 19.4 A efectos de la modificación del presente Acuerdo de Ejecución o de sus Anexos, habrá unanimidad cuando las Partes presentes y representadas lleguen a un acuerdo sobre la modificación propuesta. Por lo tanto, las Partes ausentes o no representadas no podrán impedir la adopción de una modificación del Acuerdo de Ejecución. Dicha modificación se aplicará a todas las Partes.

20 Fecha de efecto; firma; depositario

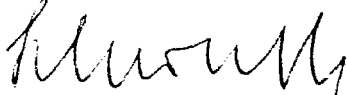
- 20.1 Para las Partes para las que haya entrado en vigor el Tratado, el presente Acuerdo de Ejecución surtirá efecto después de su firma y de la adopción de las decisiones necesarias con arreglo al artículo 34, apartado 2, del Tratado. Para las demás Partes, surtirá efecto con arreglo a lo dispuesto en el artículo 50, apartado 1, y en el artículo 51, apartado 1, del Tratado, y una vez adoptadas las decisiones necesarias con arreglo al artículo 34, apartado 2, del Tratado.
- 20.2 El presente Acuerdo de Ejecución, junto con sus Anexos, se firmará en alemán, español, francés, neerlandés e inglés, siendo todas las versiones igualmente auténticas.
- 20.3 El Gobierno de la República Federal de Alemania será el depositario del presente Acuerdo de Ejecución y de sus Anexos.

Bruselas, 5 de diciembre de 2006

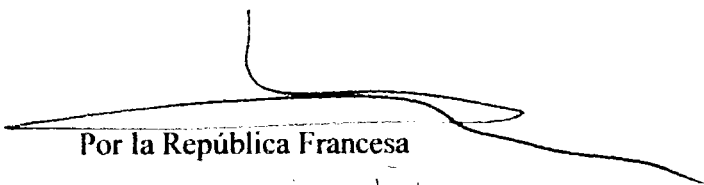
Por el Reino de Bélgica



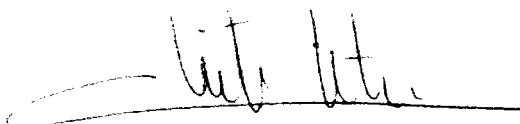
Por la República Federal de Alemania



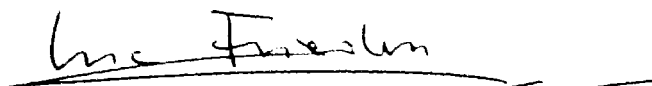
Por el Reino de España



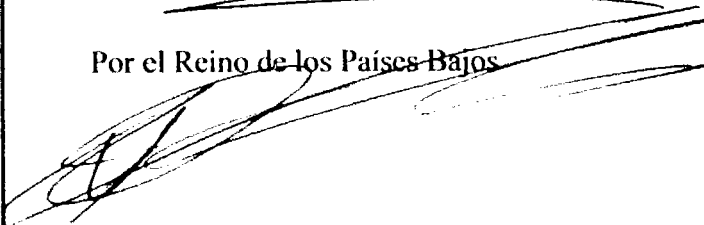
Por la República Francesa



Por el Gran Ducado de Luxemburgo



Por el Reino de los Países Bajos



Por la República de Austria



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_ty	Type of profile

	pe	
result	PRUEM_datas_res ult	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_profil e	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_hitqualit y_type	Quality of Hit
HITCOUNT	Integer	Count of matched Alleles

2.3.2. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: 1. Case "No Hit": original requesting profile sent back only; 2. 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

2.3.3. PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

2.3.4. 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

2.3.5. IPSTG_DNA_profile

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

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

2.3.6. IPSTG_DNA_ISSOL

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

Fields	Type	Description
Vwa	IPSTG_DNA_locus	Locus vwa
th01	IPSTG_DNA_locus	Locus th01
D21s11	IPSTG_DNA_locus	Locus d21s11

Fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
Amelogenin	IPSG_DNA_locus	Locus amelogenin

2.3.7. 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

2.3.8. 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 DN's 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 (Trans European Services for Telematics between Administrations) 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.

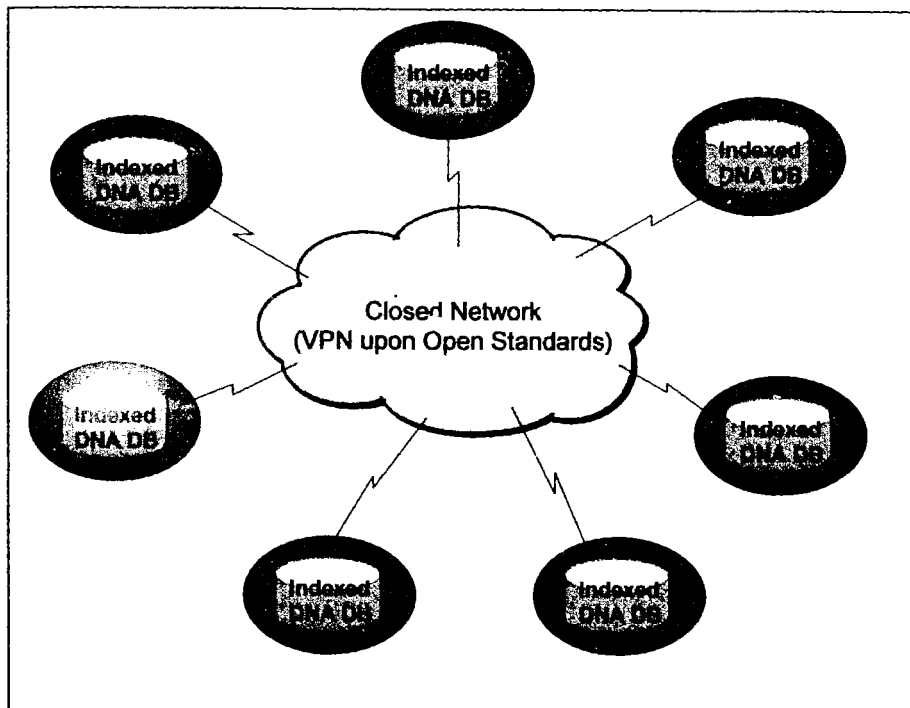
Each Party will decide which option to take by itself. This access scheme should be accepted by future acceding States to the Treaty.

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.

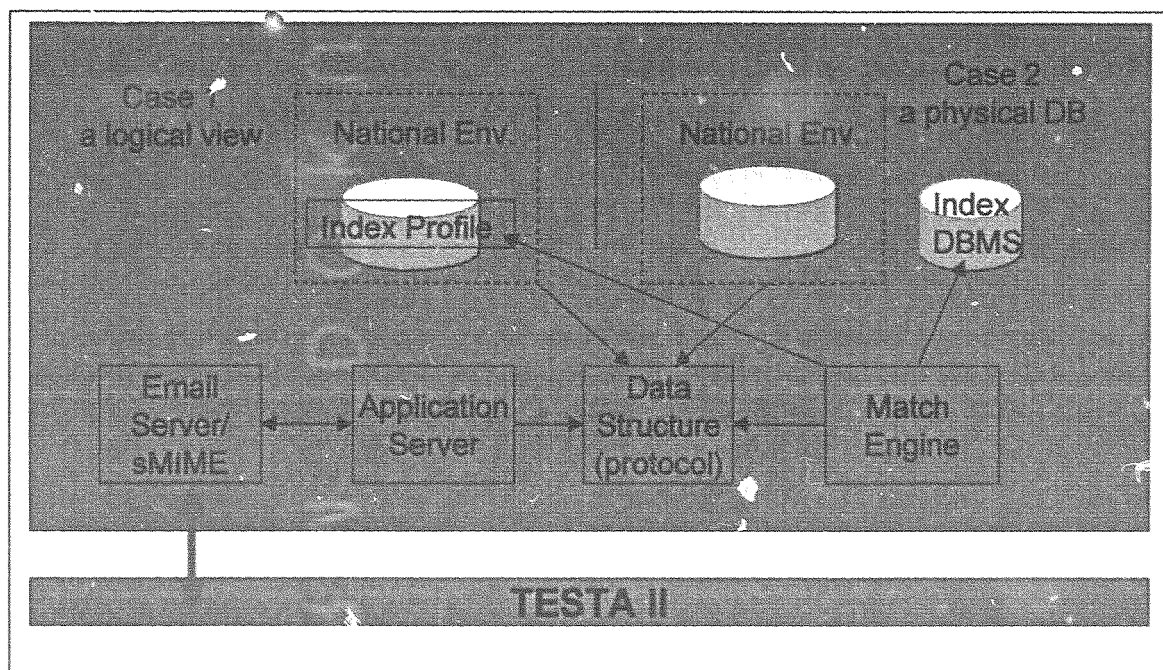
Because of sMIME's easy integration into national IT infrastructure at all Parties' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal "Proof of Concept" in a more efficient way and reducing costs the open standard JavaMail API is however 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 (Java Cryptographic Extension) 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 eXtensible Markup Language (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

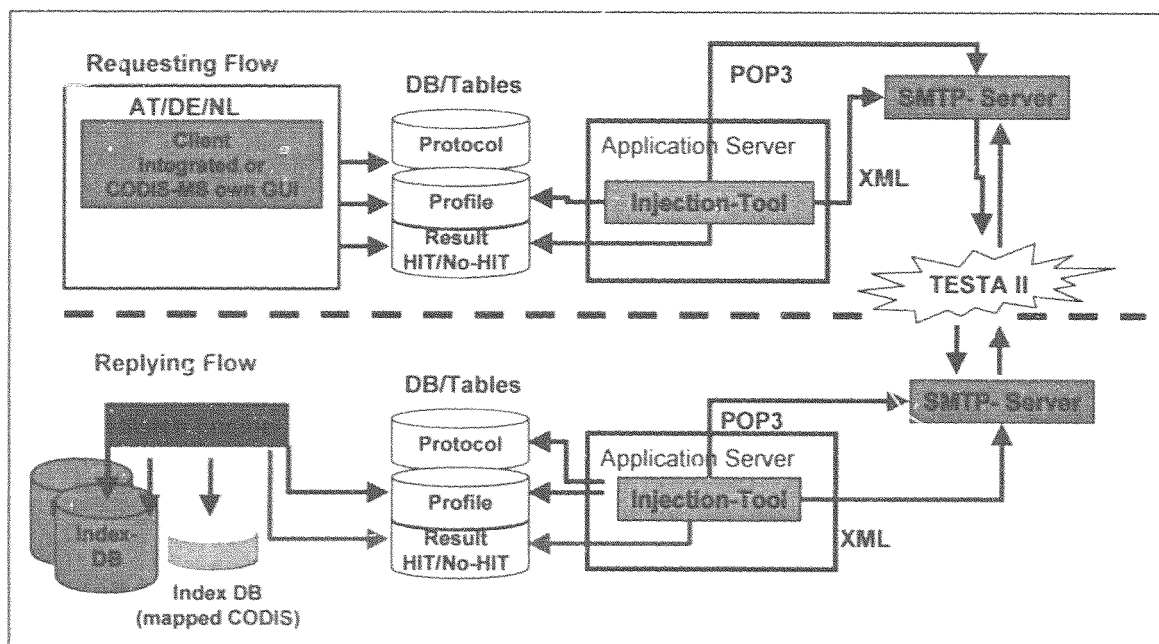
Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has however certain drawbacks. Administering a large number of client machines can involve a diversity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

6.3 JDBC

Java DataBase Connectivity (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



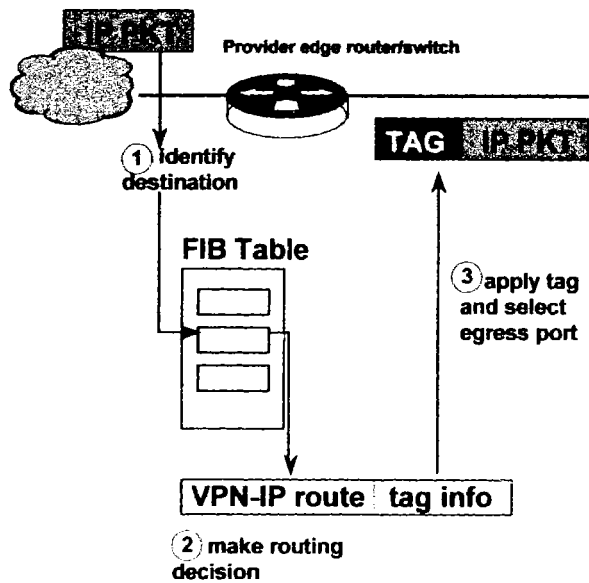
7. Communication Environment

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 Domain Name Services (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 Mail Transfer Protocol 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 **Post Office Protocol 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
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	<i>dna.pruem.at.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.at.eu-admin.net</i>	
Belgium	<i>dna.pruem.be.eu-admin.net</i>	Setting up a secure local link to the existing TESTA II access point
	<i>fp.pruem.be.eu-admin.net</i>	
Germany	<i>dna.pruem.de.eu-admin.net</i>	Using the existing TESTA II national access points
	<i>fp.pruem.de.eu-admin.net</i>	
Spain	<i>dna.pruem.es.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.es.eu-admin.net</i>	
France	<i>dna.pruem.fr.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.fr.eu-admin.net</i>	
Luxemburg	<i>dna.pruem.lu.eu-admin.net</i>	Using the existing TESTA II national access point
	<i>fp.pruem.lu.eu-admin.net</i>	
The Netherlands	<i>dna.pruem.nl.eu-admin.net</i>	Intending to establish a new TESTA II access point at the NFI
	<i>fp.pruem.nl.eu-admin.net</i>	

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-1, 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 minutiae 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 alphanumeric 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 alphanumeric 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 minutiae 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 minutiae 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: YYSSSSSSSA

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 MEAN TIME (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 represent 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 field 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 field 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 field contains the SQN (field 2.008) transmitted by an MPS or MMS transaction.

4.1.11 FIELD 2.015: MISCELLANEOUS IDENTIFICATION NUMBER (MN4)

This field 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

Numeric Code (1-3)	Meaning (5-128)
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
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: MINUTIAE RECORD

Type-9 records shall contain ASCII text describing minutiae 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 MINUTIAE 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.

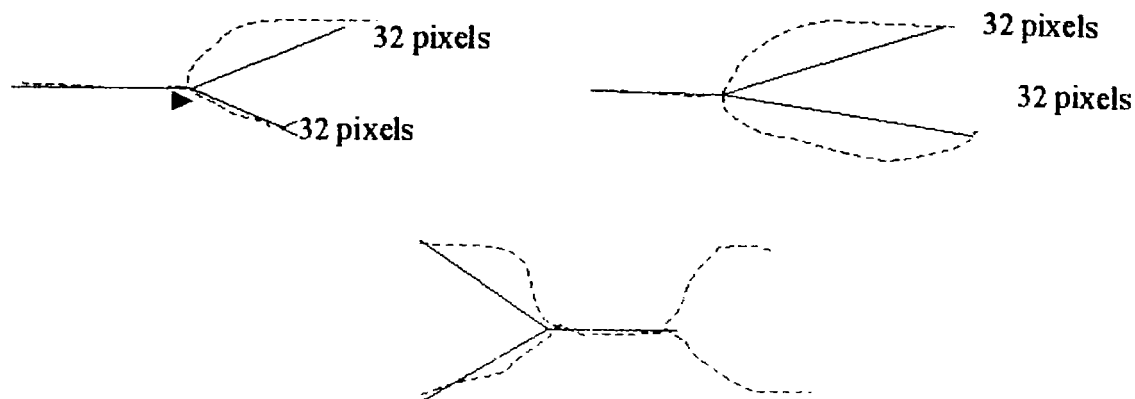
The position or location of a minutia representing a ridge ending shall be the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the three legs of the valley area were thinned down to a single-pixel-wide skeleton, the point of the intersection is 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 MINUTIAE 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 minutiae 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: MINUTIAE 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 minutiae 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 minutiae record.

6.2.15 FIELD 9.136: NUMBER OF MINUTIAE

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

6.2.16 FIELD 9.137: FINGER MINUTIAE 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	Con d. code	Field Numbe r	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
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	--	--	--	--	--	--

Ident	Con d. code	Field Numbe r	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
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	Con d. cod e	Field Numb er	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	Con d. cod e	Field Numb er	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 (mm²)	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 Position¹Description

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

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

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.

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
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}
DO M	M	1.013	Domain Name	AN	1.013: INT- I{US}4.22{GS}
GM T	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 2{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}99999 9{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	A	2.015:A{GS}

			Identification Number		
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}
SNQ	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 ¹	Remarks	Prüm Y/N ²
Data relating to vehicles			
Licence number	M		Y
Chassis number / VIN	M		Y
Party of registration	M		Y
Make	M	(D.1 ³) e.g. Ford, Opel, Renault etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
Nature of the vehicle / EU Category Code	M	(J) mopeds, motorbikes, cars etc.	Y

2.2.2 Complete data set

Item	M/O ⁴	Remarks	Prüm Y/N
Data relating to holders of the vehicle			
(C.1⁵)			
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,	Y

¹ M = mandatory when available in national register, O = optional

² All the attributes specifically allocated by the Parties are indicated with Y.

³ Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

⁴ M = mandatory when available in national register, O = optional

⁵ Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

Item	M/O ⁴	Remarks	Prüm Y/N
		Zip code, Place of residence, Party of residence etc., and the Address in printable format will be communicated	
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
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

Item	M/O ⁴	Remarks	Prüm Y/N
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 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.

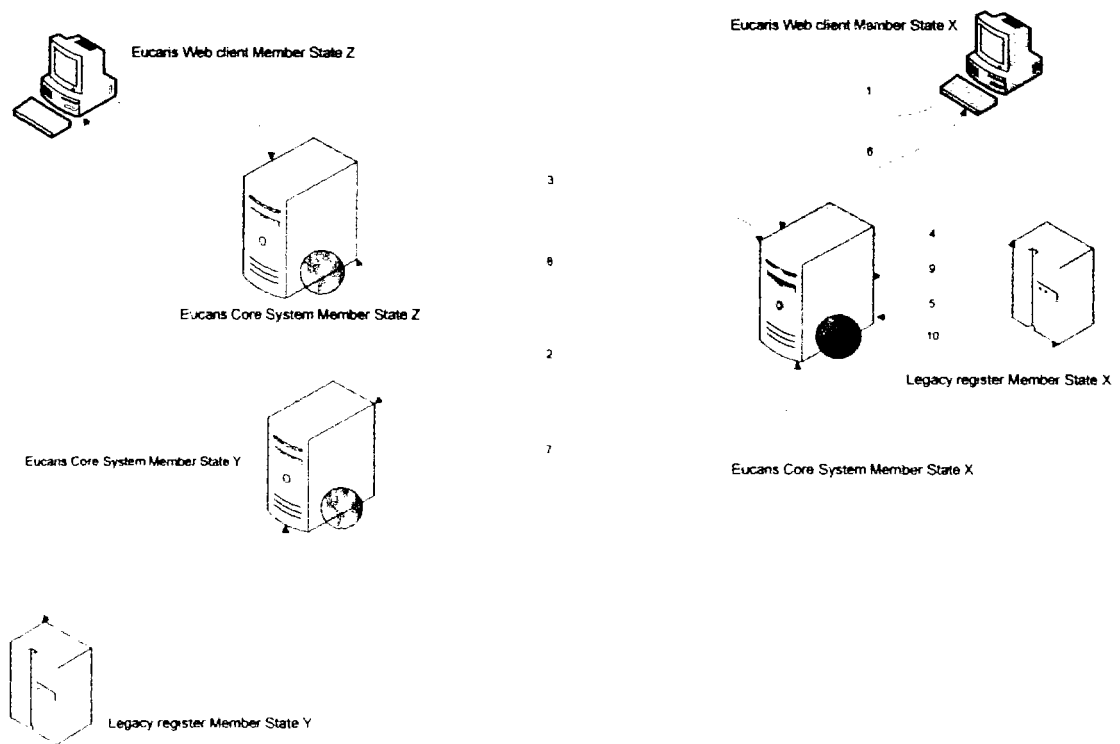


Figure : Message types for logging

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.

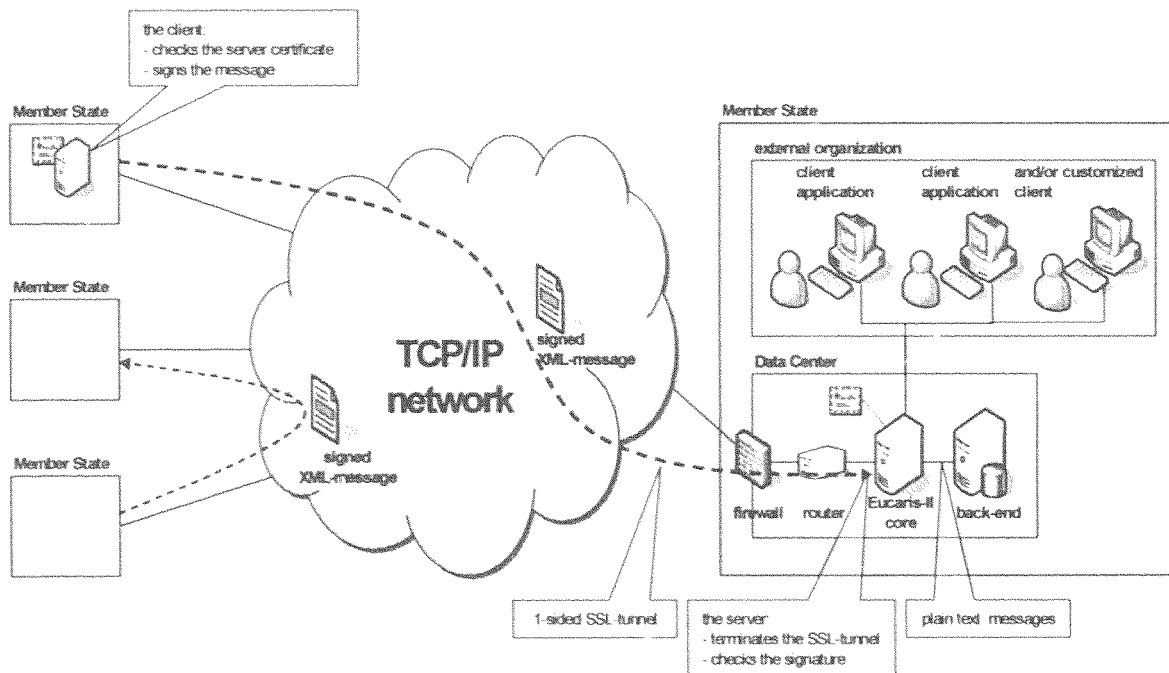
Annex C.3

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/O⁶	Remark
Network concept	M	The concept is an “any-to-any” communication.
Physical network	M	TESTA
Core application	M	<p>The core application of EUCARIS has to be used to connect to the other Parties. The following functionality is offered by the core:</p> <ul style="list-style-type: none"> ▪ 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.
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 acceptance 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.

⁶ M = mandatory to use or to comply with O = optional to use or to comply with

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.

Nr.	Description
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.
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

Nr.	Description
	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.
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

Nr.	Description
	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.

Nr.	Description
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

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	<u>Help.div@m</u> <u>obilit.fgov.be</u> (DIV) <u>Help.ict@m</u> <u>obilit.fgov.be</u> (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	+34915371883	+34913191228	

	de Seguridad (Ministry of Interior)	+34915371884 +34915372056 +34915372057 +34915372058	+34913191645 +34913197389	ceplic@ses.m ir.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@l.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)

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@l.lka.bwl.de e 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 : 04 68 83 79 10 Tel : 05 59 20 93 60 Fax : 05 59 20 59 34 E-mail : ccpd-hendaye@interieur.gouv.fr ccpd-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 Article 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

Tel.: +49 (0) 1888 681-1077

Fax.: +49 (0) 1888 681-2926

Mail: poststelle@bmi.bund.de

- für die Bundespolizei:
Abteilung für Angelegenheiten der
Bundespolizei

Tel.: +49 (0) 1888 681-0

Fax: +49 (0) 1888 681-1829

Mail: poststelle@bmi.bund.de

Alt-Moabit 101D
D-10559 Berlin

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

Niedersachsen (NI)

Niedersächsisches Ministerium für Inneres und Sport

Tel.: +49 (0) 511 120-6112

Fax.: +49 (0) 511 120-6150

Mail: kvl@mi.niedersachsen.de

Lavesallee 6
D-30169 Hannover

Nordrhein-Westfalen (NW)

Innenministerium Nordrhein-Westfalen

Tel.: +49 (0)211 871

3340/3341/3342/3343/3344

Fax.: +49 (0)211 871 3231

Mail: lagezentrum@im.nrw.de

- Lagezentrum -

Haroldstraße 5
40190 Düsseldorf

Rheinland-Pfalz (RP)

Ministerium des Innern und für Sport

Tel.: +49 (0)6131 16 3599

Fax.: +49 (0)6131 16 3600

Mail: lagezentrum@ism.rlp.de

- Lagezentrum -

Schillerplatz 3-5
55116 Mainz

Saarland (SL)

Ministerium für Inneres, Familie, Frauen und Sport

Tel.: +49 (0) 681 962-1260 bis 1263

Fax.: +49 (0) 681 962-1265

Mail: lagezentrum@innensaarland.de

Leitstelle, Lagezentrum-
c/o Landespolizeidirektion
Mainzer Str 134 -136
66121 Saarbrücken

Baden-Württemberg (BW)

Innenministerium Baden-Württemberg

Tel.: +49 (0)711 231 3333

Fax.: +49 (0)711 231 3399

Mail: lagezentrum@im.bwl.de

Lagezentrum

Dorotheenstraße 6
70173 Stuttgart

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
Lagezentrum 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 Wiesbaden

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

Tel.: +49 351 564 3775 oder 3776

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

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 or 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

Competent authorities: Police and Royal Constabulary (Koninglijke Marechaussee)

Memberstates	Organisation	Central point of contact	Telephone number Fax number E-mail
AUSTRIA BELGIUM GERMANY FRANCE LUXEMBURG	Korps Landelijke Politie Diensten (KLPD) Department for Conflict and	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	Crisismanagement Koninklijke Marechaussee (Royal Constabulary) Commander of National and Foreign Squads	Kamp Nieuw Millingen Postbus 59 3886 ZH Garderen	Tel: (0031)(0)577455766 Fax:(0031)(0)577455763
-------	---	--	---

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:

Gabinete 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: <u>LPK-O@polizei.gv.at</u>
	Landespolizeikommando Salzburg - Landesleitzentrale		Tel.: +43 (0) 59133 50-2222 Fax: +43 (0) 59133 50-1009 Mail: <u>LPK-S@polizei.gv.at</u>
	Landespolizeikommando Tirol - Landesleitzentrale		Tel.: +43 (0) 59133 70-2222 Fax: +43 (0) 59133 70-1009 Mail: <u>LPK-T@polizei.gv.at</u>
	Landespolizeikommando Vorarlberg - Landesleitzentrale		Tel.: +43 (0) 59133-80-2222 Fax: +43 (0) 59133-80-1009 Mail: <u>LPK-V@polizei.gv.at</u>
OTHER PARTYS	Federal Ministry of the Interior, Division II – General Directorate for Public		Phone: +431-53126-3200 or -3775 Fax: +431-53126-3120 e-mail: <u>bmi-II-EKC-</u>

	Security, Operations and Crisis Coordination Centre		<u>Permanenzdienst@bmi. gv.at</u>
--	---	--	---------------------------------------

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/LANGEMARK-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/HENSIÉS/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
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/	+ 32 (0) 80 28.14.10

		BURG-REULAND/ SANKT-VITH	
LUXEM- BOURG	PZ 5298 SUD- LUXEMBOURG	AUBANGE /MESSANCY/ MUSSON/SAINT-LEGER	+ 32 (0) 63 38.02.54
	PZ 5297	ARLON / ATPERT / 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/VIELSAL M	+32 (0)84 31.03.11
	PZ 5291 EIFEL	AMEL /BULLINGEN/ BUTGENBACH/ BURG-REULAND/ SANKT-VITH	+ 32 (0) 80 28.14.10
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
	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@l.lka.bwl.de ccpd2-offenbourg.ddpaf-67@interieur.gouv.fr or : fabien.taglang@interieur.gouv.fr (Chef détachement P.N.)
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.fr cpd-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	Local contactpoints of the police (Police of the Länder	All municipalities at the borders with the Prüm	

(AT,FR, LU, BE, NL)	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	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 LU XEMBOURG
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
-------------	--------------	-----------------	--------------------------------

<p>BELGIUM GERMANY</p>	<p>Korps Landelijke Politiediensten (KLPD) (Police) Bureau Conflict-en Crisisbeheersing</p> <p>Or:</p> <p>Local contactpoints of the regional policeforces</p> <p>In the event of a border crossing, the competent regional Police Communications Centre (Gemeenschappelijk meldkamer) must be informed immediately</p>	<p>Hoofdstraat 54 Postbus 100 3970 AC Driebergen</p>	<p>E-mail</p> <p>Tel: (0031)(0)343536366 Fax:(0031)(0)343518180 E- mail:ccb.klpd@klpd.politi e.nl</p>
----------------------------	---	--	---

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

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

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 HEAD QUARTERS	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

REGION	UNIT	ADRESS	TELEFONO	FAX
Pais Vasco	Headquarters of San Sebastián	C/ José M 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
Cataluna	Headquarters of Girona	C/ Sant Pau, 2	34.972.220025	34.972.201149
Cataluna	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:

+ 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:

ceplic@ses.mir.es

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:

1. 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.
2. 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 robbery 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 be 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. 1^{er}. 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 1^{er}:

- 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 immobiliser 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 1^{er} opérant d'office ou sur les ordres de leurs supérieurs hiérarchiques ou sur la réquisition de l'autorité judiciaire peuvent immobiliser 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 entflozene 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 special 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 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 rifle, 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 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 deprivation 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 ammunition 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 grenades 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 of his 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 deportation 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 unconscious 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 surveillance

Article 31

1. After receiving the consent of the assistant district attorney, the officer can subject the detainee to permanent video surveillance.
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 surveillance and shall make a record of the permanent video surveillance.

§ 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 published 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 reposes 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 reposes 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.

Accord d'exécution

du Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm, Allemagne, le 27 mai 2005.

Section 1 : Objectif et définitions

1. Objectif

Conformément à l'article 44 du Traité, l'objectif du présent Accord d'exécution est de déterminer les conditions nécessaires à la mise en oeuvre administrative et technique et à l'exécution du Traité.

2. Définitions

Aux fins du présent Accord d'exécution :

- 2.1 Le terme « Traité » désigne le Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm, Allemagne, le 27 mai 2005 ;
- 2.2 Le terme « Partie » désigne une Partie Contractante au Traité qui a signé le présent Accord d'exécution ;
- 2.3 Les procédures de « consultation », de « comparaison » ou de « consultation par comparaison » visées aux articles 3, 4 et 9 du Traité signifient les procédures par lesquelles il est établi qu'il y a une concordance entre, respectivement, les données ADN ou les données dactyloscopiques communiquées par une Partie et les données ADN ou les données dactyloscopiques contenues dans les bases de données d'une, de plusieurs, ou de toutes les autres Parties ;
- 2.4 L'expression « profil ADN » désigne un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon ADN humain analysé, c'est-à-dire la forme chimique particulière issue de différents segments ADN (loci) ;
- 2.5 L'expression « partie non codante de l'ADN » désigne les zones chromosomes ne contenant aucune expression génétique, c'est-à-dire non connues pour fournir des informations sur des caractéristiques héréditaires spécifiques ;
- 2.6 L'expression « « données indexées ADN » désigne un profil ADN et les données non ADN spécifiques y associées ;
- 2.7 L'expression « données spécifiques non ADN » comprend :
 - 2.7.1 un code d'identification ou un chiffre permettant aux Parties, s'il y a concordance, de rechercher des données à caractère personnel et / ou

- d'autres informations dans leurs bases de données afin de les fournir à une, plusieurs ou toutes les autres Parties, conformément à l'article 5 du Traité ;
- 2.7.2 un code désignant la Partie afin d'indiquer l'origine nationale du profil ADN, et
- 2.7.3 un code pour indiquer le type de profil ADN tel que déclaré par les Parties conformément à l'article 2, paragraphe 2 du Traité ;
- 2.8 L'expression « profil ADN non identifié » désigne le profil ADN obtenu à partir de cellules humaines provenant d'enquêtes pénales et appartenant à une personne non encore identifiée ;
- 2.9 L'expression « profil ADN indexé » est une expression technique et désigne le profil ADN d'une personne identifiée figurant aux fichiers nationaux d'analyses ADN conformément à l'article 2, paragraphe 3 du Traité ;
- 2.10 L'expression « données dactyloscopiques » désigne les images d'empreintes digitales, images d'empreintes digitales cachées, d'empreintes de paumes de mains, d'empreintes de paumes de mains cachées, ainsi que des modèles de telles images (*menus détails*), dans la mesure où ils sont stockés et traités dans une base de données automatisée ;
- 2.11 L'expression « demande de suivi » désigne la demande d'une Partie adressée à une, plusieurs ou toutes les autres Parties en cas de concordance entre des données ADN ou dactyloscopiques comparées, afin d'obtenir d'autres données à caractère personnel et d'autres informations conformément aux articles 5 et 10 du Traité ;
- 2.12 L'expression « données des registres d'immatriculation des véhicules » désigne l'ensemble de données spécifiées à l'Annexe C.1 que les Parties ont accepté de se rendre mutuellement disponibles aux fins de la procédure de consultation automatisée définie ci-après au point 2.13 ;
- 2.13 L'expression « consultation automatisée » désigne la consultation en ligne afin d'interroger, conformément à l'article 33, paragraphe 1, point 2 du Traité, les bases de données d'une, de plusieurs, ou de toutes les autres Parties ;
- 2.14 L'expression « système ex article 12 » désigne l'ensemble des mesures techniques et aspects fonctionnels, tels que réseaux, interfaces et systèmes de sécurité, établis en vue de l'échange de données des registres d'immatriculation des véhicules conformément à l'article 12 du Traité ;
- 2.15 Le terme « EUCARIS » désigne le système d'information européen concernant les véhicules et les permis de conduire instauré par le Traité EUCARIS, signé à Luxembourg le 29 juin 2000 ;
- 2.16 L'expression « au cas par cas » désigne, par référence à l'article 3, paragraphe 1, à l'article 9, paragraphe 1 et à l'article 12, paragraphe 1 du Traité, une seule enquête

ou un seul dossier de poursuites pénales ; si cette enquête ou ce dossier concernent plus d'un profil ADN, d'une donnée dactyloscopique ou d'une donnée des registres d'immatriculation des véhicules, ces profils ou ces données peuvent être transmis ensemble en une seule demande ;

- 2.17 L'expression « raison de la demande ou de la transmission de données » désigne, pour l'application de l'article 39 du Traité, une indication qui permet d'établir un lien évident entre une demande déterminée et le cas individuel correspondant qui a motivé la demande ;
- 2.18 L'expression « réseau de communication TESTA II » désigne les « Services transeuropéens pour la télématique entre Administrations » gérés par la Commission européenne, ainsi que toute version modifiée de ce réseau.

Section 2 : Profils ADN

3. Composition et comparaison de profils ADN

- 3.1 Aux fins de l'application de l'article 2 du Traité, les données indexées ADN qui sont échangées conformément aux dispositions du Traité sont composées d'un profil ADN et de données spécifiques non ADN.
- 3.2 Un ensemble de spécifications techniques communes, incluant les règles de concordance, les algorithmes et les numéros de code des Parties tels que définis aux Annexes A, sera mis en place et déployé aux points de contact nationaux des Parties et appliqué à toutes les demandes et réponses liées aux consultations et comparaisons de profils ADN visées au point 3.1.
- 3.3 Les profils ADN seront comparés sur la base de marqueurs d'ADN communs tels que définis à l'Annexe A.1. Chaque profil ADN transmis pour consultation ou comparaison automatisée par la Partie requérante sera comparé avec chaque profil ADN mis à disposition pour comparaison par les Parties requises, conformément à l'article 2, paragraphes 2 et 3 du Traité.
- 3.4 Les Parties utilisent les normes existantes telles que l'ensemble européen de référence (European Standard Set, ESS) ou le Groupe standard de loci d'Interpol (Interpol Standard Set of Loci, ISSOL).

4. Règles relatives aux demandes et réponses ADN

- 4.1 La demande de consultation ou de comparaison automatisée, visée aux articles 3 et 4 du Traité, inclut uniquement les informations suivantes :
- 4.1.1 le code Partie de la Partie requérante ;
- 4.1.2 la date, l'heure et le numéro de référence de la demande ;

- 4.1.3 les profils ADN et leurs données spécifiques non ADN ;
 - 4.1.4 le type de profils ADN transmis (profil ADN non identifié ou profil ADN indexé).
- 4.2 Les Parties font le nécessaire pour que les demandes soient totalement conformes aux conditions imposées par les déclarations faites en vertu de l'article 2, paragraphe 3 du Traité et reproduites à l'Annexe A.3.
- 4.3 La réponse (rapport de concordance) à la demande visée au point 4.1 sera transmise au point de contact national de la Partie requérante afin de déterminer si une demande de suivi peut être présentée. Un rapport de concordance contient uniquement les informations suivantes :
- 4.3.1 l'indication précisant s'il y a eu une ou plusieurs concordances (hit) ou non (no-hit) ;
 - 4.3.2 la date, l'heure et le numéro de référence de la demande ;
 - 4.3.3 la date, l'heure et le numéro de référence de la réponse ;
 - 4.3.4 le code Partie de la Partie requise ;
 - 4.3.5 les données spécifiques non ADN de la Partie requérante et de la Partie requise ;
 - 4.3.6 le type de profils ADN transmis (profils ADN non identifiés ou profils ADN indexés) ;
 - 4.3.7 en cas de comparaison automatisée conformément à l'article 4 du Traité, le profil ADN ayant fait l'objet d'une concordance.
- 4.4 La notification automatisée d'une concordance (« hit ») est effectuée uniquement à condition que la consultation ou la comparaison automatisée ait mis en évidence une concordance basée sur un minimum de loci tel que spécifié à l'Annexe A.1. Dans le cas d'une consultation automatisée conformément à l'article 3 du Traité, à des fins de vérification, les points de contact nationaux des Parties prennent les mesures appropriées conformément à leur droit national.

5. Réseau de communication pour la transmission des données ADN

Les échanges électroniques de données ADN entre les Parties sont effectués via le réseau de communication "TESTA II" selon les spécificités techniques telles que décrites à l'Annexe A.5.

6. Mesures de contrôle de qualité

Les Parties prennent les mesures appropriées afin de garantir l'intégrité des profils ADN mis à la disposition des autres Parties ou transmis pour comparaison. Ces mesures doivent être conformes aux normes internationales, telles que l'ISO 17025. Les aspects d'expertise médico-légale de ces profils ADN doivent respecter les caractéristiques définies à l'Annexe A.1.

Section 3 : Données dactyloscopiques

7. Transmission de données dactyloscopiques

- 7.1 Aux fins de l'application de l'article 9 du Traité, les Parties établissent un accès technique mutuellement accessible à leurs « systèmes automatisés d'identification par empreintes digitales » (dénommés ci-après "AFIS").
- 7.2 Les systèmes mentionnés au point 7.1 incluent uniquement les systèmes automatisés d'identification dactyloscopique établis en vue de la prévention et de la poursuite d'infractions pénales. Des données incluses dans des fichiers administratifs ne doivent pas être transmises.
- 7.3 La numérisation des données dactyloscopiques et leur transmission aux autres Parties s'effectue selon le format de données précisé dans le document de contrôle d'interface (« Interface Control Document-ICD ») tel que défini à l'Annexe B.1. Chaque Partie s'assure que les données dactyloscopiques transmises par les autres Parties peuvent être comparées aux données indexées de son propre « AFIS ».
- 7.4 Les données indexées mentionnées à l'article 9 du Traité permettent d'établir la correspondance univoque d'une personne ou d'une affaire criminelle, ainsi que l'identification de la Partie requérante.

8. Consultation et transmission des résultats

- 8.1 Les Parties s'assurent que les données dactyloscopiques transmises sont de qualité appropriée aux fins de comparaison par l'AFIS. La Partie requise contrôle sans délai la qualité des données dactyloscopiques transmises par un procédé entièrement automatisé. Dans l'éventualité de données non appropriées pour une comparaison automatisée, la Partie requise en informe immédiatement la Partie requérante.
- 8.2 La Partie requise effectue les consultations dans l'ordre chronologique d'arrivée des demandes. Les demandes doivent être traitées dans les 24 heures par un procédé entièrement automatisé. La Partie requérante, peut, si sa législation nationale l'exige, demander le traitement accéléré de ces consultations. La Partie requise effectue ces consultations immédiatement. Si les délais ne peuvent pas être respectés pour des raisons dont la Partie requise n'est pas responsable, il est nécessaire d'effectuer la comparaison sans délai dès que les obstacles ont été levés.
- 8.3 La Partie requise veille à ce que le système puisse transmettre sans délai de façon entièrement automatisée chaque réponse de concordance (hit) ou de non concordance (no-hit) à la Partie requérante. En cas de concordance (hit), elle transmet les données dactyloscopiques et les données indexées visées à l'article 9, paragraphe 2 du Traité pour toutes les concordances entre des données dactyloscopiques.

9. Réseau de communication pour la transmission des données dactyloscopiques

L'échange électronique de données dactyloscopiques entre les Parties doit être effectué via le réseau de communication « TESTA II », conformément aux spécifications techniques définies à l'Annexe A.5.

10. Définition et capacités de la consultation automatisée des données dactyloscopiques

- 10.1 La quantité maximale des différents types de données dactyloscopiques (candidats) admise par transmission pour vérification est déterminée à l'Annexe B.2.
- 10.2 Les capacités maximales de consultation journalières de chaque Partie concernant les données dactyloscopiques de personnes identifiées sont déterminées à l'Annexe B.3.
- 10.3 Les capacités maximales de consultation journalières de chaque Partie concernant les traces dactyloscopiques sont déterminées à l'Annexe B.4.

Section 4 : Données relatives aux registres d'immatriculation de véhicules

11. Procédure de consultation et transmission des données

- 11.1 Aux fins de l'article 12 du Traité, les Parties établissent un réseau de points de contact nationaux afin d'effectuer des consultations automatisées dans leurs registres d'immatriculation de véhicules respectifs. Les conditions techniques relatives aux échanges de données sont déterminées à l'Annexe C.3.
- 11.2 Sans préjudice des dispositions du Traité, et en tenant compte notamment des dispositions des articles 38 et 39, les Parties, agissant respectivement en qualité d'Etat requérant ou requis, organisent le mode de fonctionnement de leurs points de contact nationaux, de bonne foi eu égard aux principes et dispositions du Traité.
- 11.3 Les Parties qui optent pour une procédure de demande entièrement automatisée doivent s'assurer que toutes leurs demandes passent par leur point de contact national prévu par le Traité, qui doit être placé sous le contrôle d'un fonctionnaire responsable.

12. Réseau de communication pour la transmission des données des registres d'immatriculation de véhicules

- 12.1 Aux fins de l'échange électronique des données des registres d'immatriculation de véhicules, les Parties décident d'utiliser le réseau de communication « TESTA II » et

une version de l'application du logiciel EUCARIS spécialement adaptée pour les besoins du système ex article 12, ainsi que toute version modifiée de ces deux systèmes.

12.2 La répartition des frais afférents à la gestion et à l'utilisation du système ex article 12, y compris les coûts liés à la technologie EUCARIS, doit être discutée et approuvée annuellement.

13. Mesures techniques et organisationnelles pour garantir la protection des données personnelles et la sécurité des données

Les spécifications techniques de la consultation automatisée telle que visée à l'article 38, paragraphe 2 du Traité relatives à la protection, à la sécurité, à la confidentialité et à l'intégrité des données, à l'encryptage du réseau, aux procédures d'authentification et aux procédures de contrôle pour la recevabilité de consultations automatisées sont détaillées à l'Annexe C.2.

Section 5 : Coopération policière

14. Interventions communes

14.1 Au moyen d'un descriptif de mission, deux ou plusieurs Parties peuvent organiser une intervention commune telle que prévue à l'article 24 du Traité. Avant le commencement de l'intervention, elles déterminent, verbalement ou par écrit, les dispositions relatives aux modalités opérationnelles, telles que :

- a) les autorités compétentes des Parties concernées par le descriptif de mission ;
- b) le but précis de l'intervention ;
- c) l'Etat d'accueil où l'intervention aura lieu ;
- d) la zone géographique de l'Etat d'accueil où l'intervention aura lieu ;
- e) la période couverte par le descriptif de mission ;
- f) l'assistance spécifique à fournir par l'Etat d'envoi à l'Etat d'accueil, y compris des fonctionnaires ou d'autres agents de l'autorité publique, des éléments matériels ou financiers ;
- g) les fonctionnaires participant à l'intervention ;
- h) le fonctionnaire responsable de l'intervention ;
- i) les attributions des fonctionnaires et autres agents de l'autorité publique de l'Etat d'envoi dans l'Etat d'accueil pendant l'intervention ;
- j) les armes, munitions et équipements particuliers que les fonctionnaires de l'Etat d'envoi peuvent utiliser pendant l'intervention conformément aux règles prévues à l'Annexe D.3 ;
- k) les modalités logistiques relatives au transport, à l'hébergement et à la sécurité ;
- l) la prise en charge des frais de l'intervention commune, si elle diffère des dispositions prévues à l'article 46 du Traité ;
- m) tout autre élément nécessaire le cas échéant.

14.2 Les autorités compétentes de chacune des Parties peuvent demander la mise en place d'une intervention commune. A l'Annexe D.1, chaque Partie peut définir les procédures relatives à l'introduction des demandes. Si aucune procédure n'est définie, un point de contact national conformément à l'Annexe D.1 est désigné afin d'aider les autres Parties à adresser leurs demandes aux autorités compétentes.

15. Interventions transfrontalières en cas de danger présent

15.1. Les autorités à aviser sans délai conformément à l'article 25, paragraphe 3 du Traité, figurent à l'Annexe D.2.

15.2 Toute modification des coordonnées de ces autorités est communiquée dès que possible aux points de contact des autres Parties également répertoriés à l'Annexe D.2.

16. Port et utilisation des armes, munitions et équipements

A l'Annexe D.3, chaque Partie répertorie les armes, munitions et équipements particuliers dont le port est interdit conformément à l'article 28, paragraphe 1, 3^{ème} phrase du Traité, les armes, munitions et équipements particuliers dont l'utilisation est interdite conformément à l'article 28, paragraphe 2 du Traité, ainsi que les aspects pratiques visés à l'article 28, paragraphe 5 du Traité.

Section 6 : Dispositions générales

17. Evaluation de l'application et de la mise en œuvre du Traité et de l'Accord d'exécution

17.1 L'évaluation de l'application et de la mise en œuvre techniques et administratives du Traité et de l'Accord d'exécution est réalisée par le groupe de travail commun, tel que prévu par l'article 43, paragraphe 2 du Traité, ou par tout groupe technique de travail spécifique mandaté à cet effet par le groupe de travail commun. Une telle évaluation peut être exécutée sur demande d'une des Parties.

17.2 Les modalités de consultation et de comparaison automatisées de données ADN et dactyloscopiques seront évaluées, sauf décision contraire du groupe de travail commun, six mois après le début des activités menées dans le cadre du présent Accord d'exécution. Pour les données des registres d'immatriculation de véhicules cette première évaluation aura lieu trois mois après le début des activités. Par la suite, de telles évaluations peuvent avoir lieu sur demande d'une des Parties, conformément à l'article 43 du Traité.

17.3 Les autorités compétentes pour la journalisation conformément à l'article 39, paragraphe 2 du Traité procèdent à des vérifications aléatoires à la fréquence et dans la mesure nécessaires pour permettre une évaluation efficace de la légitimité des consultations automatisées effectuées par les points de contact nationaux respectifs, conformément aux articles 3, 9 et 12 du Traité.

18. Disponibilité des échanges de données automatisés

Les Parties feront tous les efforts raisonnables afin de maintenir l'échange en ligne automatisé de données ADN, dactyloscopiques et de registres d'immatriculation de véhicules sur la base d'une disponibilité 24 heures/24 et 7 jours/7. Dans l'éventualité d'une défaillance technique, les points de contact des Parties concernées s'informent mutuellement dès que possible et s'accordent sur un moyen alternatif temporaire de communication, conformément à tout autre instrument juridique applicable. L'échange automatisé des données doit être remis en service aussi rapidement que possible.

19. Modification de l'Accord d'exécution et de ses Annexes

19.1 Des modifications du présent Accord d'exécution et de ses Annexes peuvent être proposées par toute Partie. De telles propositions sont communiquées à toutes les autres Parties.

19.2 Si la modification proposée concerne les dispositions de l'Accord d'exécution, elle est adoptée par décision du Comité des ministres conformément à l'article 43, paragraphe 1 du Traité.

19.3 Si la modification proposée concerne une ou plusieurs des Annexes de l'Accord d'exécution, elle est adoptée par le groupe de travail commun conformément à l'article 43, paragraphe 2 du Traité.

19.4 Aux fins de la modification du présent Accord d'exécution ou de ses Annexes, l'unanimité est atteinte lorsque les Parties présentes et représentées approuvent la modification proposée. En conséquence, l'absence ou la non représentation de Parties ne peuvent empêcher l'adoption d'une modification de l'Accord d'exécution. Cette modification vaut pour toutes les Parties.

20. Prise d'effet, signature, dépositaire

20.1 Pour les Parties pour lesquelles le Traité est entré en vigueur, le présent Accord d'exécution prend effet après sa signature et après l'adoption des décisions nécessaires prévues à l'article 34, paragraphe 2 du Traité. Pour les autres Parties, il prend effet conformément à l'article 50, paragraphe 1, ou à l'article 51, paragraphe 1

du Traité, selon le cas, ainsi qu'après l'adoption des décisions nécessaires prévues à l'article 34, paragraphe 2 du Traité.

20.2 Le présent Accord d'exécution ainsi que ses annexes sera signé en langues allemande, espagnole, française, néerlandaise et anglaise, les cinq textes faisant également foi.

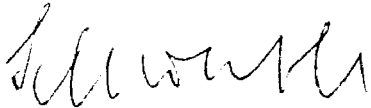
20.3 Le Gouvernement de la République fédérale d'Allemagne agit en qualité de dépositaire du présent Accord d'exécution et de ses Annexes.

Bruxelles, le 5 décembre 2006

Pour le Royaume de Belgique



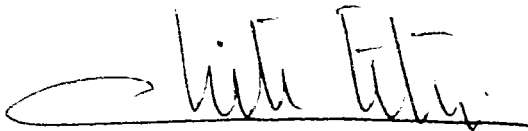
Pour la République fédérale d'Allemagne



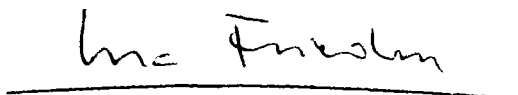
Pour le Royaume d'Espagne



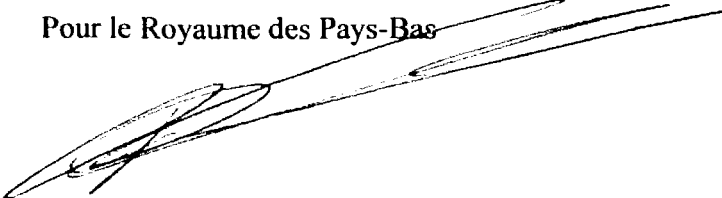
Pour la République française



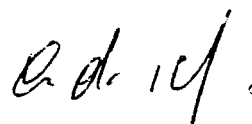
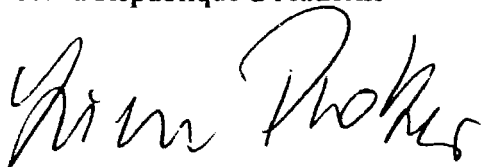
Pour le Grand-Duché de Luxembourg,



Pour le Royaume des Pays-Bas



Pour la République d'Autriche



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. For 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_ty	Type of profile

	pe	
result	PRUEM_datas_res ult	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_profil e	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_hitqualit y_type	Quality of Hit
HITCOUNT	Integer	Count of matched Alleles

2.3.2. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: <ol style="list-style-type: none"> 1. Case "No Hit": original requesting profile sent back only; 2. 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

2.3.3. PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

2.3.4. 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

2.3.5. IPSPG_DNA_profile

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

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

2.3.6. IPSPG_DNA_ISSOL

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

Fields	Type	Description
Vwa	IPSPG_DNA_locus	Locus vwa
th01	IPSPG_DNA_locus	Locus th01
D21s11	IPSPG_DNA_locus	Locus d21s11

Fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
Amelogenin	IPSG_DNA_locus	Locus amelogenin

2.3.7. 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

2.3.8. 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 (Trans European Services for Telematics between Administrations) 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.

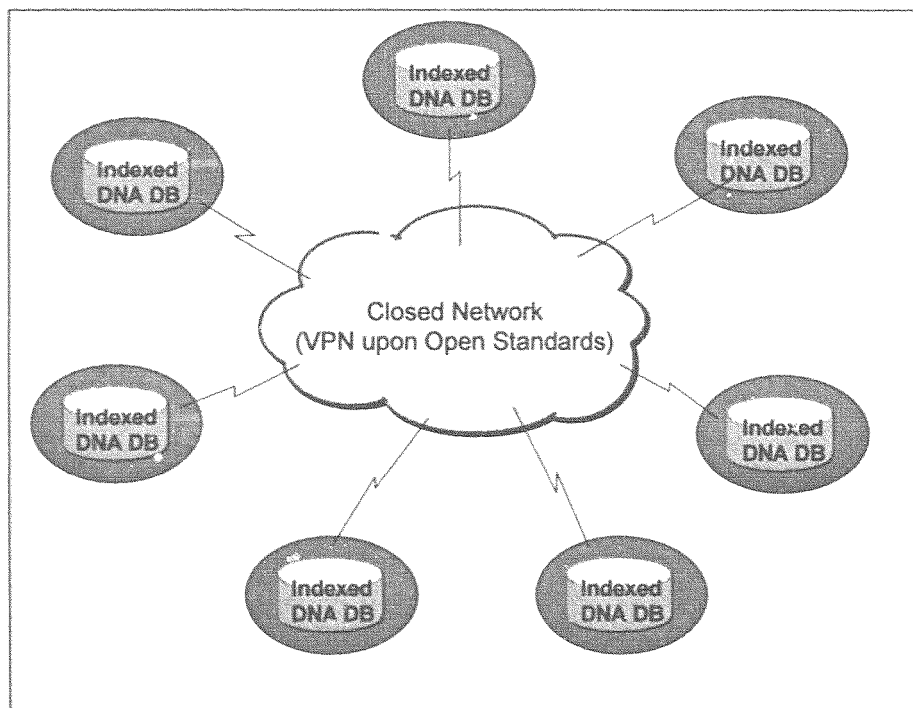
Each Party will decide which option to take by itself. This access scheme should be accepted by future acceding States to the Treaty.

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.

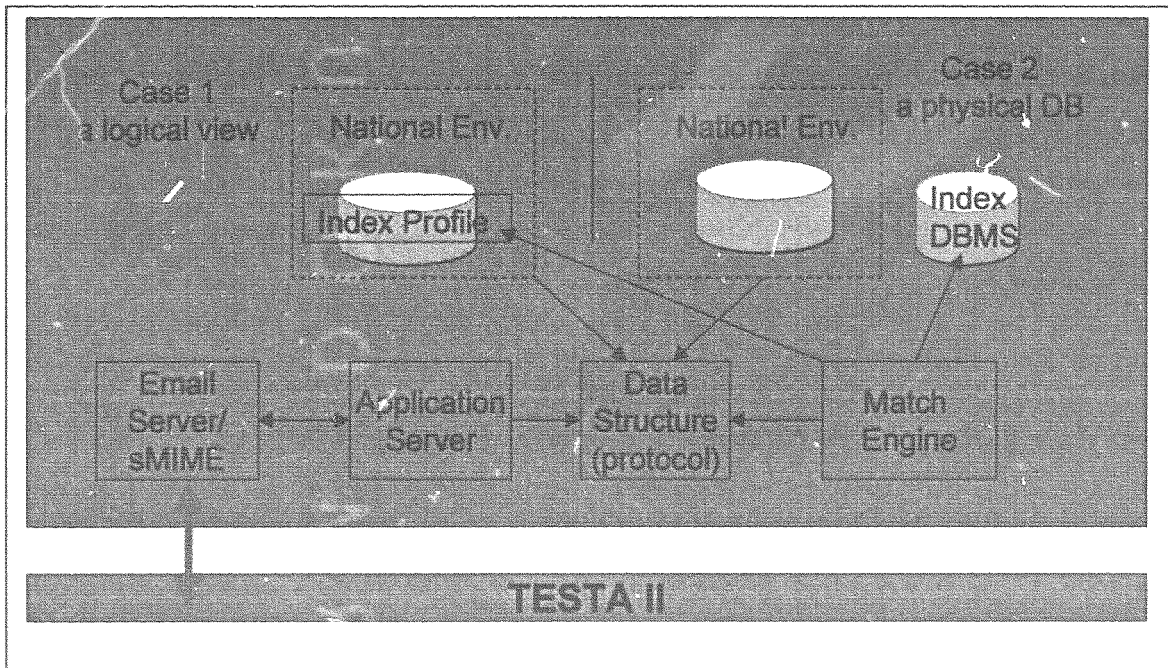
Because of sMIME's easy integration into national IT infrastructure at all Parties' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal "Proof of Concept" in a more efficient way and reducing costs the open standard JavaMail API is however 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 (Java Cryptographic Extension) 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 eXtensible Markup Language (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

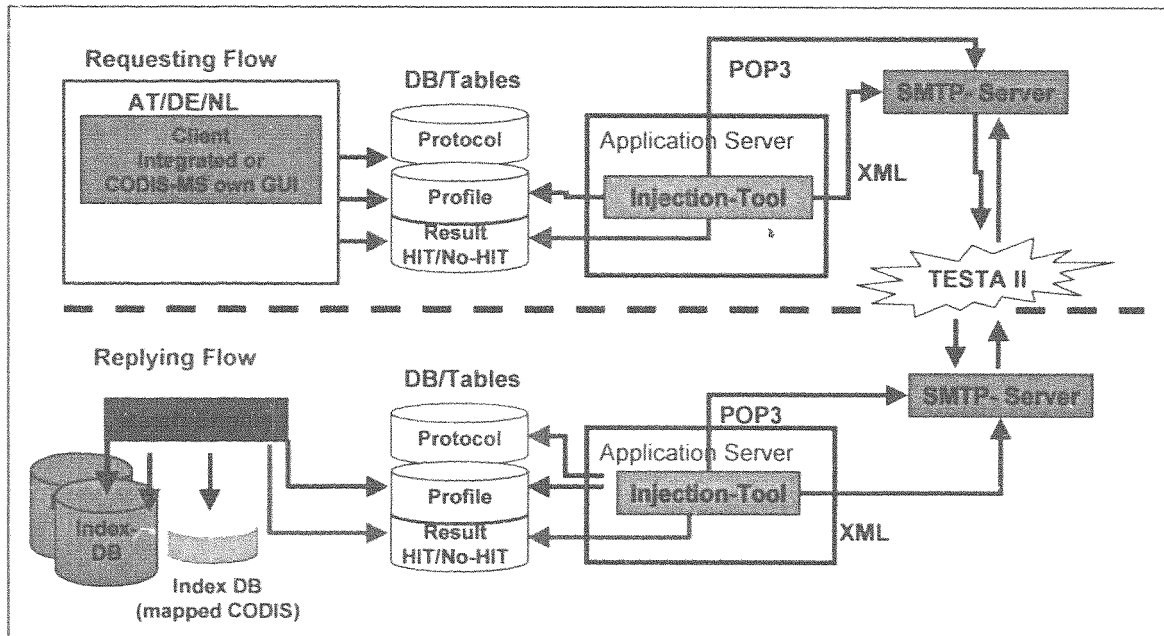
Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has however certain drawbacks. Administering a large number of client machines can involve a diversity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

6.3 JDBC

Java DataBase Connectivity (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



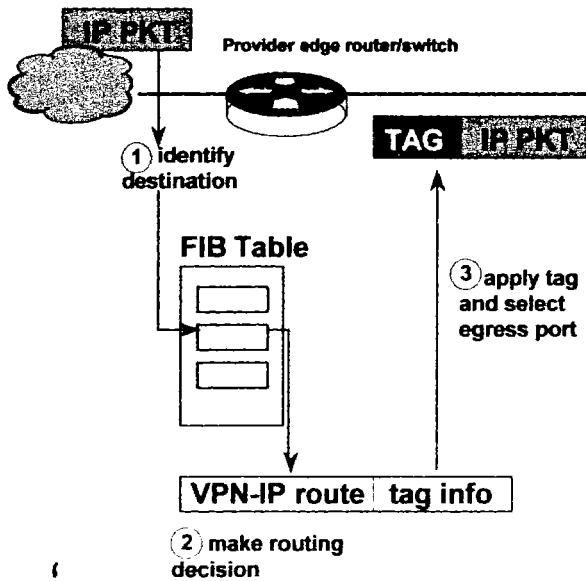
7. Communication Environment

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 Domain Name Services (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 Mail Transfer Protocol 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 **Post Office Protocol 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
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	<i>dna.pruem.at</i> .eu-admin.net	Using the existing TESTA II national access point
	<i>fp.pruem.at</i> .eu-admin.net	
Belgium	<i>dna.pruem.be</i> .eu-admin.net	Setting up a secure local link to the existing TESTA II access point
	<i>fp.pruem.be</i> .eu-admin.net	
Germany	<i>dna.pruem.de</i> .eu-admin.net	Using the existing TESTA II national access points
	<i>fp.pruem.de</i> .eu-admin.net	
Spain	<i>dna.pruem.es</i> .eu-admin.net	Using the existing TESTA II national access point
	<i>fp.pruem.es</i> .eu-admin.net	
France	<i>dna.pruem.fr</i> .eu-admin.net	Using the existing TESTA II national access point
	<i>fp.pruem.fr</i> .eu-admin.net	
Luxemburg	<i>dna.pruem.lu</i> .eu-admin.net	Using the existing TESTA II national access point
	<i>fp.pruem.lu</i> .eu-admin.net	
The Netherlands	<i>dna.pruem.nl</i> .eu-admin.net	Intending to establish a new TESTA II access point at the NFI
	<i>fp.pruem.nl</i> .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 minutiae 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 alphanumeric 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 minutiae 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 minutiae 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 MEAN TIME (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 represent 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".