BESCHLUSS 2008/616/JI DES RATES

vom 23. Juni 2008

zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf Artikel 33 des Beschlusses 2008/615/JI des Rates ([1]),

auf Initiative der Bundesrepublik Deutschland,

nach Stellungnahme des Europäischen Parlaments ([2]),

in Erwägung nachstehender Gründe:

(1) Der Rat hat am 23. Juni 2008 den Beschluss 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, angenommen.

(2) Mit dem Beschluss 2008/615/JI werden die wesentlichen Elemente des Vertrags vom 27. Mai 2005 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 (nachstehend „Prümer Vertrag" genannt), in den Rechtsrahmen der Europäischen Union überführt.

(3) Gemäß Artikel 33 des Beschlusses 2008/615/JI nimmt der Rat die für die Durchführung des Beschlusses 2008/615/JI auf Unionsebene erforderlichen Maßnahmen nach dem Verfahren des Artikels 34 Absatz 2 Buchstabe c Satz 2 des Vertrags über die Europäische Union an. Diese Maßnahmen haben sich auf die Durchführungsvereinbarung vom 5. Dezember 2006 zur verwaltungsmäßigen und technischen Umsetzung des Prümer Vertrags zu stützen.

(4) Dieser Beschluss legt die unabdingbaren gemeinsamen normativen Vorschriften für die verwaltungsmäßige und technische Umsetzung der im Beschluss 2008/615/JI genannten Formen der Zusammenarbeit fest. Der Anhang zu diesem Beschluss enthält die Durchführungsbestimmungen technischer Art. Außerdem wird ein gesondertes Handbuch, das ausschließlich Sachinformationen der Mitgliedstaaten enthält, vom Generalsekretariat des Rates erstellt und laufend auf dem neuesten Stand gehalten.

(5) Unter Berücksichtigung der technischen Kapazitäten werden Routine-Abfragen neuer DNA-Profile grundsätzlich in Form von Einzelabfragen vorgenommen; hierfür werden auf technischer Ebene geeignete Lösungen erarbeitet —

BESCHLIESST:

KAPITEL 1

ALLGEMEINES

Artikel 1

Ziel

Mit diesem Beschluss sollen die erforderlichen verwaltungsmäßigen und technischen Bestimmungen für die Umsetzung des Beschlusses 2008/615/JI festgelegt werden, insbesondere für den automatisierten Austausch von DNA-Daten, daktyloskopischen Daten und Fahrzeugregisterdaten gemäß Kapitel 2 jenes Beschlusses sowie andere Formen der Zusammenarbeit gemäß Kapitel 5 desselben Beschlusses.

Artikel 2

Begriffsbestimmungen

Im Sinne dieses Beschlusses bezeichnet der Ausdruck

a) „Abruf" und „Abgleich" gemäß den Artikeln 3, 4 und 9 des Beschlusses 2008/615/JI jenes Verfahren, mit dem festgestellt wird, ob eine Übereinstimmung der DNA-Daten oder daktyloskopischen Daten, die von einem Mitgliedstaat übermittelt wurden, mit den DNA-Daten oder daktyloskopischen Daten, die in den Datenbanken eines, mehrerer oder aller Mitgliedstaaten gespeichert sind, vorliegt;

b) „automatisierter Abruf" gemäß Artikel 12 des Beschlusses 2008/615/JI ein Online-Zugangsverfahren, um auf die Datenbanken einer, mehrerer oder aller Mitgliedstaaten zugreifen zu können;

c) „DNA-Profil" einen Buchstaben- beziehungsweise Zahlencode, der eine Reihe von Identifikationsmerkmalen des nicht codierenden Teils einer analysierten menschlichen DNA-Probe, d. h. der speziellen Molekularstruktur an den verschiedenen DNA-Loci, abbildet;

d) „nicht codierender Teil der DNA" die Chromosomenbereiche, die keine genetische Information, d. h. keine Hinweise auf funktionale Eigenschaften eines Organismus, enthalten;

([1]) Siehe Seite 1 dieses Amtsblatts.
([2]) Stellungnahme vom 21. April 2008 (noch nicht im Amtsblatt veröffentlicht).

e) „DNA-Fundstellendatensatz“ ein DNA-Profil und eine Kennung;

f) „DNA-Personenprofil“ das DNA-Profil einer identifizierten Person;

g) „offene Spur“ ein DNA-Profil einer noch nicht identifizierten Person, das aus Spuren im Zuge der Ermittlung von Straftaten gewonnen wurde;

h) „Notiz“ eine von einem Mitgliedstaat in seiner nationalen Datenbank an einem DNA-Profil angebrachte Markierung, aus der hervorgeht, dass auf den Abruf oder Abgleich eines anderen Mitgliedstaats hin bereits eine Übereinstimmung mit diesem DNA-Profil festgestellt wurde;

i) „daktyloskopische Daten“ Fingerabdrücke, Fingerabdruckspuren, Handabdrücke, Handabdruckspuren und Schablonen (*Templates*) derartiger Abdrücke (codierte Minutien), wenn diese in einer automatisierten Datenbank gespeichert und verarbeitet werden;

j) „Fahrzeugregisterdaten“ den Datensatz gemäß Kapitel 3 des Anhangs zu diesem Beschluss;

k) „Einzelfall“ gemäß Artikel 3 Absatz 1 Satz 2, Artikel 9 Absatz 1 Satz 2 und Artikel 12 Absatz 1 des Beschlusses 2008/615/JI einen einzelnen Ermittlungs- oder Strafverfolgungsakt. Enthält ein solcher Ermittlungs- oder Strafverfolgungsakt mehr als ein DNA-Profil, daktyloskopisches Datum oder Fahrzeugregisterdatum, so können diese Daten gemeinsam als eine Anfrage übermittelt werden.

KAPITEL 2

GEMEINSAME BESTIMMUNGEN FÜR DEN DATENAUSTAUSCH

Artikel 3

Technische Spezifikationen

Die Mitgliedstaaten beachten bei allen Anfragen und Rückmeldungen bezüglich der Abrufe und Abgleiche von DNA-Profilen, daktyloskopischen Daten und Fahrzeugregisterdaten gemeinsame technische Spezifikationen. Diese technischen Spezifikationen sind im Anhang dieses Beschlusses festgelegt.

Artikel 4

Kommunikationsnetzwerk

Der elektronische Austausch von DNA-Daten, daktyloskopischen Daten und Fahrzeugregisterdaten zwischen den Mitgliedstaaten erfolgt unter Verwendung des Kommunikationsnetzwerks TESTA II (Transeuropäische Telematikdienste zwischen Behörden) sowie dessen Fortentwicklungen.

Artikel 5

Verfügbarkeit des automatisierten Datenaustauschs

Die Mitgliedstaaten treffen alle notwendigen Vorkehrungen, damit der automatisierte Abruf oder Abgleich von DNA-Daten, daktyloskopischen Daten und Fahrzeugregisterdaten 24 Stunden täglich und 7 Tage pro Woche möglich ist. Im Fall einer technischen Störung informieren die nationalen Kontaktstellen der Mitgliedstaaten einander umgehend und vereinbaren für die Zwischenzeit einen alternativen Informationsaustausch gemäß den geltenden rechtlichen Regelungen. Der automatisierte Datenaustausch ist so schnell wie möglich wieder herzustellen.

Artikel 6

Kennungen für DNA-Daten und daktyloskopische Daten

Die in Artikel 2 und Artikel 8 des Beschlusses 2008/615/JI genannten Kennungen bestehen aus einer Kombination folgender Elemente:

a) Code, der es den Mitgliedstaaten im Fall einer Übereinstimmung ermöglicht, personenbezogene Daten und sonstige Informationen in ihren Datenbanken abzurufen, um sie einem, mehreren oder allen Mitgliedstaaten gemäß Artikel 5 oder Artikel 10 des Beschlusses 2008/615/JI zu übermitteln,

b) Code, der die nationale Herkunft des DNA-Profils beziehungsweise des daktyloskopischen Datums anzeigt, und

c) im Zusammenhang mit DNA-Daten Code, der den Typ des DNA-Profils anzeigt.

KAPITEL 3

DNA-DATEN

Artikel 7

Grundsätze des DNA-Datenaustauschs

(1) Die Mitgliedstaaten verwenden für den DNA-Datenaustausch bestehende Standards, wie beispielsweise ESS (European Standard Set) oder ISSOL (Interpol Standard Set of Loci).

(2) Das Übermittlungsverfahren beim automatisierten Abruf und Abgleich von DNA-Profilen erfolgt im Wege einer dezentralen Struktur.

(3) Es werden geeignete Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität der an andere Mitgliedstaaten weitergeleiteten Daten, einschließlich ihrer Verschlüsselung, getroffen.

(4) Die Mitgliedstaaten treffen die notwendigen Maßnahmen, um die Integrität der den anderen Mitgliedstaaten zur Verfügung gestellten oder zum Abgleich übermittelten DNA-Profile zu garantieren und um zu gewährleisten, dass diese Maßnahmen mit internationalen Standards, wie zum Beispiel der Norm ISO 17025, übereinstimmen.

(5) Die Mitgliedstaaten verwenden Mitgliedstaatencodes gemäß der Norm ISO 3166-1 alpha-2.

Artikel 8

Regeln für Anfragen und Rückmeldungen bei DNA-Daten

(1) Die Anfrage zwecks eines automatisierten Abrufs oder Abgleichs gemäß Artikel 3 oder 4 des Beschlusses 2008/615/JI enthält ausschließlich die folgenden Informationen:

a) den Mitgliedstaatencode des anfragenden Mitgliedstaats;

b) das Datum, den Zeitpunkt und die Referenznummer der Anfrage;

c) die DNA-Profile und deren Kennungen;

d) die Typen übermittelter DNA-Profile (offene Spuren oder DNA-Personenprofile);

e) Informationen, die für die Steuerung der Datenbanksysteme und die Qualitätssicherung für die automatisierten Abrufverfahren erforderlich sind.

(2) Die Rückmeldung (Vergleichsbericht) auf die Anfrage gemäß Absatz 1 enthält ausschließlich folgende Informationen:

a) die Angabe, ob eine oder mehrere Übereinstimmungen (Treffer) oder keine Übereinstimmungen (keine Treffer) vorliegen;

b) das Datum, den Zeitpunkt und die Referenznummer der Anfrage;

c) das Datum, den Zeitpunkt und die Referenznummer der Rückmeldung;

d) die Mitgliedstaatencodes des anfragenden und des die Anfrage empfangenden Mitgliedstaats;

e) die Kennungen des anfragenden und des die Anfrage empfangenden Mitgliedstaats;

f) den Typ der übermittelten DNA-Profile (offene Spuren oder DNA-Personenprofile);

g) die angefragten und übereinstimmenden DNA-Profile;

h) die Informationen, die für die Steuerung der Datenbanksysteme und die Qualitätssicherung für die automatisierten Abrufverfahren erforderlich sind.

(3) Die automatisierte Information über das Vorliegen einer Übereinstimmung erfolgt nur, wenn der automatisierte Abruf oder Abgleich eine Übereinstimmung eines Minimums an Loci ergeben hat. Dieses Minimum an Loci ist in Kapitel 1 des Anhangs zu diesem Beschluss festgelegt.

(4) Die Mitgliedstaaten stellen sicher, dass die Anfragen mit den gemäß Artikel 2 Absatz 3 des Beschlusses 2008/615/JI abgegebenen Erklärungen übereinstimmen. Diese Erklärungen sind in dem Handbuch gemäß Artikel 18 Absatz 2 dieses Beschlusses wiedergegeben.

Artikel 9

Übermittlungsverfahren beim automatisierten Abruf von offenen Spuren gemäß Artikel 3 des Beschlusses 2008/615/JI

(1) Wird beim Abruf mit einer offenen Spur in der nationalen Datenbank keine Übereinstimmung oder aber eine Übereinstimmung mit einer offenen Spur festgestellt, kann eine Übermittlung der offenen Spur an die Datenbanken aller anderen Mitgliedstaaten erfolgen; und werden beim Abruf mit dieser offenen Spur Übereinstimmungen mit DNA-Personenprofilen und/oder offenen Spuren in den Datenbanken der anderen Mitgliedstaaten festgestellt, erfolgt eine automatische Mitteilung dieser Übereinstimmungen und eine Übermittlung der DNA-Fundstellendatensätze an den anfragenden Mitgliedstaat; kann keine Übereinstimmung in den Datenbanken der anderen Mitgliedstaaten festgestellt werden, wird dies dem anfragenden Mitgliedstaat automatisch mitgeteilt.

(2) Wird beim Abruf mit einer offenen Spur eine Übereinstimmung in den Datenbanken der anderen Mitgliedstaaten festgestellt, kann jeder betroffene Mitgliedstaat dies in seiner nationalen Datenbank mit einer entsprechenden Notiz vermerken.

Artikel 10

Übermittlungsverfahren beim automatisierten Abruf von DNA-Personenprofilen gemäß Artikel 3 des Beschlusses 2008/615/JI

Wird beim Abruf mit einem DNA-Personenprofil in der nationalen Datenbank keine Übereinstimmung mit einem DNA-Personenprofil oder aber eine Übereinstimmung mit einer offenen Spur festgestellt, kann eine Übermittlung dieses DNA-Personenprofils an die Datenbanken aller anderen Mitgliedstaaten erfolgen; und werden beim Abruf mit diesem DNA-Personenprofil Übereinstimmungen mit DNA-Personenprofilen und/oder offenen Spuren in den Datenbanken der anderen Mitgliedstaaten festgestellt, erfolgt eine automatische Mitteilung dieser Übereinstimmungen und eine Übermittlung der DNA-Fundstellendatensätze an den anfragenden Mitgliedstaat; kann keine Übereinstimmung in den Datenbanken der anderen Mitgliedstaaten festgestellt werden, so wird dies dem anfragenden Mitgliedstaat automatisch mitgeteilt.

Artikel 11

Übermittlungsverfahren beim automatisierten Abgleich von offenen Spuren gemäß Artikel 4 des Beschlusses 2008/615/JI

(1) Werden beim Abgleich mit offenen Spuren Übereinstimmungen in den Datenbanken anderer Mitgliedstaaten mit DNA-Personenprofilen und/oder offenen Spuren festgestellt, erfolgt eine automatische Mitteilung dieser Übereinstimmungen und eine Übermittlung der DNA-Fundstellendatensätze an den anfragenden Mitgliedstaat.

(2) Werden bei dem Abgleich mit offenen Spuren Übereinstimmungen in den Datenbanken anderer Mitgliedstaaten mit offenen Spuren oder DNA-Personenprofilen festgestellt, kann jeder betroffene Mitgliedstaat dies in seiner nationalen Datenbank mit einer entsprechenden Notiz vermerken.

KAPITEL 4

DAKTYLOSKOPISCHE DATEN

Artikel 12

Grundsätze des Austauschs daktyloskopischer Daten

(1) Die Digitalisierung der daktyloskopischen Daten und ihre Übermittlung an die anderen Mitgliedstaaten erfolgen in einem einheitlichen Datenformat, wie in Kapitel 2 des Anhangs zu diesem Beschluss festgelegt.

(2) Jeder Mitgliedstaat stellt sicher, dass die von ihm übermittelten daktyloskopischen Daten für einen Abgleich anhand der automatisierten Fingerabdruck-Identifizierungssysteme (AFIS) von ausreichender Qualität sind.

(3) Das Übermittlungsverfahren beim Austausch daktyloskopischer Daten erfolgt im Wege einer dezentralen Struktur.

(4) Es werden geeignete Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität der an andere Mitgliedstaaten übermittelten daktyloskopischen Daten, einschließlich ihrer Verschlüsselung, getroffen.

(5) Die Mitgliedstaaten verwenden Mitgliedstaatencodes gemäß der Norm ISO 3166-1 alpha-2.

Artikel 13

Abrufkapazitäten für daktyloskopische Daten

(1) Jeder Mitgliedstaat gewährleistet, dass seine Abrufanfragen nicht die Abrufkapazitäten überschreiten, die der die jeweilige Anfrage empfangende Mitgliedstaat angegeben hat. Die Mitgliedstaaten übermitteln dem Generalsekretariat des Rates Erklärungen gemäß Artikel 18 Absatz 2, in denen sie ihre maximalen Abrufkapazitäten pro Tag für daktyloskopische Daten von identifizierten Personen und für daktyloskopische Daten von noch nicht identifizierten Personen angeben.

(2) Die maximale Anzahl der daktyloskopischen Daten („candidates"), die pro Übermittlung zur Verifikation zugelassen werden, ist in Kapitel 2 des Anhangs zu diesem Beschluss festgelegt.

Artikel 14

Regeln für Anfragen und Rückmeldungen bei daktyloskopischen Daten

(1) Der die Anfrage empfangende Mitgliedstaat prüft unverzüglich und vollautomatisiert die Qualität der übermittelten daktyloskopischen Daten. Sind die Daten für einen automatisierten Abgleich ungeeignet, informiert dieser Mitgliedstaat den anfragenden Mitgliedstaat unverzüglich.

(2) Der die Anfrage empfangende Mitgliedstaat nimmt die Abrufe in der Reihenfolge vor, in der die Anfragen eingegangen sind. Die Anfragen müssen innerhalb von 24 Stunden vollautomatisiert bearbeitet werden. Der anfragende Mitgliedstaat kann, wenn sein innerstaatliches Recht dies vorschreibt, eine beschleunigte Bearbeitung seiner Anfragen erbitten, und der die Anfrage empfangende Mitgliedstaat nimmt dann unverzüglich die Abrufe vor. Können Fristen aufgrund höherer Gewalt nicht eingehalten werden, ist der Abgleich sofort nach Wegfall der Hindernisse durchzuführen.

KAPITEL 5

FAHRZEUGREGISTERDATEN

Artikel 15

Grundsätze des automatisierten Abrufs von Fahrzeugregisterdaten

(1) Für den automatisierten Abruf von Fahrzeugregisterdaten verwenden die Mitgliedstaaten eine Version der Softwareanwendung Eucaris (Europäisches Fahrzeug- und Führerschein-Informationssystem), die speziell für die Zwecke von Artikel 12 des Beschlusses 2008/615/JI entwickelt wurde, sowie geänderte Versionen dieser Software.

(2) Der automatisierte Abruf von Fahrzeugregisterdaten erfolgt im Wege einer dezentralen Struktur.

(3) Die Nachrichten, die über das Eucaris-System ausgetauscht werden, werden verschlüsselt übertragen.

(4) Die Datenelemente der auszutauschenden Fahrzeugregisterdaten sind in Kapitel 3 des Anhangs zu diesem Beschluss festgelegt.

(5) Bei der Anwendung von Artikel 12 des Beschlusses 2008/615/JI können die Mitgliedstaaten Abrufen im Zusammenhang mit der Bekämpfung schwerwiegender Verbrechen Vorrang verleihen.

Artikel 16

Kosten

Jeder Mitgliedstaat trägt die Kosten, die aus der Verwaltung, der Verwendung und der Pflege der in Artikel 15 Absatz 1 genannten Eucaris-Softwareanwendung entstehen.

KAPITEL 6

POLIZEILICHE ZUSAMMENARBEIT

Artikel 17

Gemeinsame Streifen sowie sonstige gemeinsame Einsatzformen

(1) Nach Maßgabe von Kapitel 5 des Beschlusses 2008/615/JI und insbesondere der Erklärungen nach Artikel 17 Absatz 4, Artikel 19 Absatz 2 und Artikel 19 Absatz 4 desselben Beschlusses benennt jeder Mitgliedstaat eine oder mehrere

Kontaktstellen, um anderen Mitgliedstaaten zu gestatten, sich an die zuständigen Behörden zu wenden, und jeder Mitgliedstaat kann seine Verfahren für die Bildung gemeinsamer Streifen und sonstiger gemeinsamer Einsatzformen, seine Verfahren für Initiativen anderer Mitgliedstaaten in Bezug auf solche Einsätze sowie andere praktische Aspekte und die operativen Modalitäten im Zusammenhang mit diesen Einsätzen festlegen.

(2) Das Generalsekretariat des Rates erstellt die Liste der Kontaktstellen, hält diese Liste auf dem neuesten Stand und unterrichtet die zuständigen Behörden über alle Änderungen dieser Liste.

(3) Die zuständigen Behörden jedes Mitgliedstaats können die Initiative zur Bildung einer gemeinsamen Einsatzform ergreifen. Vor Beginn eines spezifischen Einsatzes treffen die in Absatz 2 genannten zuständigen Behörden mündliche oder schriftliche Absprachen über Einzelheiten wie zum Beispiel

a) die für den Einsatz zuständigen Behörden der Mitgliedstaaten;

b) den spezifischen Zweck des Einsatzes;

c) den Aufnahmemitgliedstaat, in dem der Einsatz stattfindet;

d) das geografische Gebiet des Aufnahmemitgliedstaats, in dem der Einsatz stattfindet;

e) die Dauer des Einsatzes;

f) die spezifische Unterstützung, die der bzw. die Entsendemitgliedstaaten dem Aufnahmemitgliedstaat gewähren, einschließlich der Bereitstellung von Beamten oder anderen öffentlichen Bediensteten, Material und finanziellen Mitteln;

g) die am Einsatz teilnehmenden Beamten;

h) den für den Einsatz verantwortlichen Beamten;

i) die Befugnisse, die die Beamten und sonstigen Bediensteten des Entsendemitgliedstaats/der Entsendemitgliedstaaten während des Einsatzes im Aufnahmemitgliedstaat ausüben dürfen;

j) die jeweiligen Dienstwaffen, Ausrüstungsgegenstände und Munition, die die Beamten des Entsendemitgliedstaats während des Einsatzes im Einklang mit dem Beschluss 2008/615/JI verwenden dürfen;

k) die logistischen Modalitäten bezüglich Transport, Unterbringung und Sicherheit;

l) die Aufschlüsselung der Kosten des gemeinsamen Einsatzes, wenn diese von Artikel 34 Satz 1 des Beschlusses 2008/615/JI abweicht;

m) sonstige erforderliche Elemente.

(4) Die in diesem Artikel vorgesehenen Erklärungen, Verfahren und Benennungen werden in das in Artikel 18 Absatz 2 genannte Handbuch aufgenommen.

KAPITEL 7

SCHLUSSBESTIMMUNGEN

Artikel 18

Anhang und Handbuch

(1) Weitere Einzelheiten zur technischen und verwaltungsmäßigen Umsetzung des Beschlusses 2008/615/JI sind im Anhang zu diesem Beschluss aufgeführt.

(2) Das Generalsekretariat des Rates erstellt ein Handbuch, das ausschließlich Sachinformationen enthält, die die Mitgliedstaaten im Wege der Erklärungen aufgrund des Beschlusses 2008/615/JI oder aufgrund des vorliegenden Beschlusses oder im Wege von Notifizierungen an das Generalsekretariat des Rates erteilt haben, und hält dieses Handbuch laufend auf dem neuesten Stand. Das Handbuch wird in Form eines Ratsdokuments vorgelegt.

Artikel 19

Unabhängige Datenschutzbehörden

Die Mitgliedstaaten teilen dem Generalsekretariat des Rates gemäß Artikel 18 Absatz 2 dieses Beschlusses die in Artikel 30 Absatz 5 des Beschlusses 2008/615/JI genannten unabhängigen Datenschutzbehörden oder Justizbehörden mit.

Artikel 20

Vorbereitung der in Artikel 25 Absatz 2 des Beschlusses 2008/615/JI genannten Beschlüsse

(1) Der Rat fasst einen Beschluss gemäß Artikel 25 Absatz 2 des Beschlusses 2008/615/JI auf der Grundlage eines Bewertungsberichts, dem ein Fragebogen zugrunde liegt.

(2) Im Zusammenhang mit dem automatisierten Datenaustausch gemäß Kapitel 2 des Beschlusses 2008/615/JI stützt sich der Bewertungsbericht außerdem auf einen Bewertungsbesuch und einen Testlauf, der durchgeführt wird, nachdem der betreffende Mitgliedstaat das Generalsekretariat gemäß Artikel 36 Absatz 2 Satz 1 des Beschlusses 2008/615/JI unterrichtet hat.

(3) Weitere Einzelheiten zu dem Verfahren sind in Kapitel 4 des Anhangs zu diesem Beschluss festgelegt.

Artikel 21

Bewertung des Datenaustauschs

(1) Die verwaltungsmäßige, technische und finanzielle Umsetzung des Datenaustauschs nach Kapitel 2 des Beschlusses 2008/615/JI — und insbesondere die Anwendung des Mechanismus nach Artikel 15 Absatz 5 — wird regelmäßig bewertet. Bewertet werden jene Mitgliedstaaten, die den Beschluss 2008/615/JI zum Zeitpunkt der Bewertung bereits anwenden, und jene Datenkategorien, mit deren Austausch zwischen den betreffenden

Mitgliedstaaten begonnen wurde. Die Bewertung wird anhand von Berichten der betreffenden Mitgliedstaaten vorgenommen.

(2) Weitere Einzelheiten zu dem Verfahren sind in Kapitel 4 des Anhangs zum vorliegenden Beschluss festgelegt.

Artikel 22

Bezug zur Durchführungsvereinbarung zum Prümer Vertrag

Für die durch den Prümer Vertrag gebundenen Mitgliedstaaten gelten die einschlägigen Bestimmungen dieses Beschlusses und seines Anhangs, sobald sie völlig umgesetzt sind, statt der entsprechenden Bestimmungen der Durchführungsvereinbarung zum Prümer Vertrag. Alle sonstigen Bestimmungen der Durchführungsvereinbarung finden weiterhin zwischen den Vertragsparteien des Prümer Vertrags Anwendung.

Artikel 23

Umsetzung

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um diesem Beschluss innerhalb der in Artikel 36 Absatz 1 des Beschlusses 2008/615/JI genannten Frist nachzukommen.

Artikel 24

Anwendung

Dieser Beschluss wird zwanzig Tage nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* wirksam.

Geschehen zu Luxemburg am 23. Juni 2008.

Im Namen des Rates

Der Präsident

I. JARC

ANHANG

INHALT

KAPITEL 1: **Austausch von DNA-Daten**

1. ***DNA-bezogene forensische Aspekte, Abgleichsregeln und Algorithmen***

1.1. *Merkmale der DNA-Profile*

1.2. *Trefferregeln*

1.3. *Berichtsregeln*

2. ***Staatencodes der Mitgliedstaaten***

3. ***Funktionelle Analyse***

3.1. *Verfügbarkeit des Systems*

3.2. *Zweiter Schritt*

4. ***DNA-Schnittstellenbeschreibung (ICD)***

4.1. *Einleitung*

4.2. *Definition der XML-Struktur*

5. ***Anwendungs-, Sicherheits und Kommunikationsarchitektur***

5.1. *Überblick*

5.2. *Höhere Architekturebenen*

5.3. *Sicherheitsstandards und Datenschutz*

5.4. *Für den Verschlüsselungsmechanismus zu verwendende Protokolle und Standards: s/MIME und dazugehörige Softwarepakete*

5.5. *Anwendungsarchitektur*

5.6. *Für die Anwendungsarchitektur zu verwendende Protokolle und Standards*

5.7. *Kommunikationsumgebung*

KAPITEL 2: **Austausch daktyloskopischer Daten (Schnittstellenkontrolldokument)**

1. ***Übersicht über den Dateiinhalt***

2. ***Datensatz-Format***

3. ***Typ-1-Datensatz: File Header***

4. ***Typ-2-Datensatz: Beschreibender Text***

5. ***Typ-4-Datensatz: Hochauflösendes Bild in Grautönen***

6. ***Typ-9-Datensatz: Minutiendatensatz***

7. ***Typ-13-Datensatz mit Bildern von Fingerabdruck- und Handflächenabdruckspuren in variabler Auflösung***

8. ***Typ 15: Handflächenabdruck-Bilddatei mit variabler Auflösung*** *(Type-15 variable-resolution palmprint image record)*

9. ***Anlagen zu Kapitel 2 (Austausch daktyloskopischer Daten)***

9.1. *Codes der ASCII-Trennzeichen*

9.2. *Berechnung des alphanumerischen Kontrollzeichens (Check Character)*

9.3. *Zeichencodes*

9.4. *Transaktionsübersicht*

9.5. *Typ-1-Datensatz: Definitionen*

9.6. *Typ-2-Datensatz: Definitionen*

9.7. *Graustufenkomprimierungscodes*

9.8. *Mailspezifikation*

KAPITEL 3: **Austausch von Daten aus den Fahrzeugregistern**

1. ***Einheitlicher Datensatz für den automatisierten Abruf von Daten aus den Fahrzeugregistern***

1.1. *Begriffsbestimmungen*

1.2. *Abruf von Fahrzeug-/Eigentümer-/Halterdaten*

2. ***Datensicherheit***

2.1. *Allgemeines*

2.2. *Sicherheitsmerkmale in Bezug auf den Nachrichtenaustausch*

2.3. *Sicherheitsmerkmale ohne Bezug zum Nachrichtenaustausch*

3. ***Technische Bedingungen für den Datenaustausch***

3.1. *Beschreibung der Eucaris-Anwendung*

3.2. *Funktionale/nicht funktionale Anforderungen*

KAPITEL 4: **Bewertung**

1. ***Bewertungsverfahren gemäß Artikel 20 (Vorbereitung der in Artikel 25 Absatz 2 des Beschlusses 2008/615/JI genannten Beschlüsse)***

1.1. *Fragebogen*

1.2. *Testlauf*

1.3. *Bewertungsbesuch*

1.4. *Bericht an den Rat*

2. ***Bewertungsverfahren gemäß Artikel 21***

2.1. *Statistiken und Bericht*

2.2. *Überarbeitung*

3. ***Treffen von Experten***

KAPITEL 1: **Austausch von DNA-Daten**

1. ***DNA-bezogene forensische Aspekte, Abgleichsregeln und Algorithmen***

1.1. *Merkmale der DNA-Profile*

Die DNA-Profile können 24 Zahlenpaare enthalten, welche die Allele von 24 Loci (auch: Merkmalssystemen) darstellen, die auch in den DNA-Verfahren von Interpol verwendet werden. Die Bezeichnungen dieser Loci sind in der nachstehenden Tabelle aufgeführt:

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

Die 7 grau gekennzeichneten Loci in der obersten Zeile sind sowohl im gegenwärtigen „European Standard Set of Loci" (ESS) als auch im „Interpol Standard Set of Loci" (ISSOL) enthalten.

Übermittlungsregeln

Die von den Mitgliedstaaten zum Zweck der Suche und des Abgleichs zur Verfügung gestellten DNA-Profile sowie die zu Abruf- und Abgleichzwecken übermittelten DNA-Profile müssen mindestens 6 vollständig bestimmte ([1]) Loci enthalten; zusätzlich können sie je nach Verfügbarkeit weitere Loci oder Leerfelder enthalten. Die DNA-Personenprofile müssen mindestens 6 der 7 ESS-Loci enthalten. Zur Erhöhung der Treffergenauigkeit wird empfohlen, alle verfügbaren Allele in der Indexdatenbank für DNA-Profile zu speichern und für die Suche und den Abgleich zu verwenden. Jeder Mitgliedstaat sollte, so bald wie praktisch möglich, die Loci eines neuen ESS, der von der EU übernommen wurde, einführen.

Mischspuren sind nicht zulässig, so dass die Allelwerte jedes Locus aus lediglich 2 Zahlenwerten bestehen; bei Homozygoten müssen die 2 Zahlenwerte eines bestimmten Locus identisch sein.

Für Platzhalter („Wildcards") und Mikrovarianten gelten folgende Regeln:

— Jeder im DNA-Profil enthaltene nichtnumerische Wert (z. B. „o", „f", „r", „na", „nr" oder „un") mit Ausnahme von Amelogenin muss automatisch zum Datenaustausch in eine Wildcard (*) konvertiert und gegen alle Allelwerte abgeglichen werden.

— Im Profil enthaltene numerische Werte „0", „1" oder „99" müssen automatisch zum Datenaustausch in eine Wildcard (*) umgewandelt und gegen alle Allelwerte abgeglichen werden.

— Werden 3 Allele zu einem Locus angegeben, so wird das erste Allel akzeptiert und die beiden anderen Allele werden automatisch zum Datenaustausch in eine Wildcard (*) umgewandelt und gegen alle Allelwerte abgeglichen.

— Werden Wildcards für das Allel 1 oder 2 angegeben, so werden beide Permutationen des angegebenen numerischen Wertes für den gegebenen Locus gesucht (z. B. könnte 12,* eine Übereinstimmung mit 12,14 oder 9,12 ergeben).

— Pentanukleotid-Mikrovarianten (Penta D, Penta E und CD4) werden wie folgt abgeglichen:

  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

— Tetranukleotid-Mikrovarianten (die sonstigen Loci sind Tetranukleotide) werden wie folgt abgeglichen:

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

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

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

([1]) Vollständig bestimmt bzw. belegt („full designated") verweist auf die Einbeziehung seltener Allelwerte.

1.2. *Trefferregeln*

Der Vergleich von 2 DNA-Profilen erfolgt auf der Basis der Loci, für die ein Paar von Allelwerten in beiden DNA-Profilen verfügbar sind. Mindestens 6 vollständig belegte Loci (ausgenommen Amelogenin) müssen bei beiden DNA-Profilen übereinstimmen, bevor eine Hit-Antwort übermittelt wird.

Als vollständige Übereinstimmung/„Full Match" („Qualität 1") ist ein Treffer definiert, wenn alle Allelwerte der verglichenen Loci an gleicher Stelle, sowohl im Original- („requesting") als auch im Ergebnis-DNA-Profil („requested") enthalten sind. Ein „Near Match" („Qualität 2, 3 und 4") ist definiert als Übereinstimmung, bei der nur eines der verglichenen Allele abweicht. Ein „Near Match" wird nur dann akzeptiert, wenn in den beiden abgeglichenen DNA-Profilen bei mindestens 6 vollständig belegten Loci („full designated") eine vollständige Übereinstimmung besteht.

Ein „Near Match" kann folgende Gründe haben:

— einen menschlichen Tippfehler bei der Eingabe einer der DNA-Profile im Überprüfungsersuchen oder in der DNA-Datenbank,

— einen Fehler bei der Allelbestimmung („allele-determination") oder Allelbenennung („allele-calling") bei der Erstellung des DNA-Profils.

1.3. *Berichtsregeln*

Sowohl bei einer vollständigen Übereinstimmung als auch bei einem „Near Match" sowie bei einem „No Hit" erfolgt eine Rückmeldung.

Der Trefferbericht wird der anfragenden nationalen Kontaktstelle übermittelt und zudem der befragten nationalen Kontaktstelle zugeleitet (um ihr die Abschätzung der Art und Anzahl möglicher zusätzlicher Anfragen nach Personendaten und weiteren mit dem DNA-Profil verknüpften Informationen gemäß Artikeln 5 und 10 des Beschlusses 2008/615/JI zu ermöglichen).

2. ***Staatencodes der Mitgliedstaaten***

Gemäß dem Beschluss 2008/615/JI werden die folgenden Staatencodes nach dem Standard ISO 3166-1 alpha-2 zur Bildung der Domänennamen und anderer Konfigurationsparameter für den Prüm-DNA-Datenaustausch über ein geschlossenes Netzwerk verwendet.

Die aus 2 Buchstaben zusammengesetzten Mitgliedstaatencodes nach ISO 3166-1 alpha-2 gestalten sich wie folgt.

Mitgliedstaat	Code	Mitgliedstaat	Code
Belgien	BE	Luxemburg	LU
Bulgarien	BG	Ungarn	HU
Tschechische Republik	CZ	Malta	MT
Dänemark	DK	Niederlande	NL
Deutschland	DE	Österreich	AT
Estland	EE	Polen	PL
Griechenland	EL	Portugal	PT
Spanien	ES	Rumänien	RO
Frankreich	FR	Slowakei	SK
Irland	IE	Slowenien	SI
Italien	IT	Finnland	FI
Zypern	CY	Schweden	SE
Lettland	LV	Vereinigtes Königreich	UK
Litauen	LT		

3. ***Funktionelle Analyse***

3.1. *Verfügbarkeit des Systems*

Anfragen nach Artikel 3 des Beschlusses 2008/615/JI sollten in der abzufragenden Datenbank in der chronologischen Reihenfolge ihres Versandes eingehen, wobei die ersuchenden Mitgliedstaaten innerhalb von 15 Minuten nach Eingang ihrer Anfrage eine Antwort erhalten sollten.

3.2. *Zweiter Schritt*

Geht eine Treffermeldung in einem Mitgliedstaat ein, so ist es Aufgabe seiner nationalen Kontaktstelle, die Werte des zur Anfrageübermittelten Profils mit denen des bzw. der übermittelten Antwort-Profile zu vergleichen, um die Beweiskraft des Profilabgleichs zu prüfen und zu bestätigen. Zum Zwecke einer solchen Validierung können die nationalen Kontaktstellen unmittelbar miteinander Kontakt aufnehmen.

Nach der Validierung einer Übereinstimmung zwischen zwei Profilen, d. h. eines im Wege eines automatisierten Konsultationsverfahrens erzielten Treffers („Full Match" oder „Near Match"), beginnt das Amts- oder Rechtshilfeverfahren.

4. ***DNA-Schnittstellenbeschreibung (ICD)***

4.1. *Einleitung*

4.1.1. Ziele

Dieses Kapitel definiert die Anforderungen an den Austausch von DNA-Profildaten zwischen den DNA-Datenbanksystemen aller Mitgliedstaaten. Die Kopffelder wurden speziell für den Prüm-DNA-Datenaustausch bestimmt; der Datenteil des „DNA-Profils" ist im XML-Schema auf Basis des Interpol DNA-Austausch Gateways definiert.

Die Daten werden mittels SMTP (Simple Mail Transfer Protocol) und anderen zeitgemäßen Verfahren unter Nutzung eines vom Netzbetreiber bereitgestellten zentralen Mailrelay-Servers ausgetauscht. Die XML-Datei wird als Mailanhang verschickt.

4.1.2. Gültigkeitsbereich

Das vorliegende ICD definiert ausschließlich den Inhalt der Nachricht (Mail). Alle netzspezifischen und mailspezifischen Punkte werden einheitlich definiert, um eine gemeinsame technische Grundlage für den DNA-Datenaustausch zu schaffen.

Dies schließt ein:

— das Format des Subjektfelds in der Nachricht, um eine automatisierte Verarbeitung der Nachrichten zu ermöglichen,

— die Frage, ob eine Verschlüsselung des Inhalts notwendig ist und falls ja, welche Methode anzuwenden ist,

— die maximal zulässige Länge der Nachricht.

4.1.3. XML: Struktur und Grundsätze

Aufbau einer XML-Nachricht:

— Kopfteil (header part) mit Informationen über die Übermittlung,

— Datenteil (data part), der profilspezifische Informationen sowie das Profil selbst enthält.

Für Anfragen und Antworten wird dasselbe XML-Schema verwendet.

Zur vollständigen Überprüfung offener Spuren (Artikel 4 des Beschlusses 2008/615/JI) wird es möglich sein, ein Set von Profilen in einer einzigen Nachricht zu übermitteln. Die maximal zulässige Anzahl von Profilen in einer Nachricht muss festgelegt werden. Diese Zahl hängt von der maximal zulässigen Mailgröße ab und wird nach der Auswahl des Mail-Servers festgelegt werden.

Beispiel für eine XML-Nachricht:

<?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> Wiederholung der Datenstruktur bei Übermittlung mehrerer Profile (....) in einer einzigen SMTP-Nachricht; nur zulässig bei „Artikel 4"-Fällen

</datas>]

</PRUEMDNA>

4.2. *Definition der XML-Struktur*

Die folgenden Definitionen dienen der Dokumentation und der besseren Verständlichkeit; die tatsächlich verbindlichen Informationen sind in einer XML-Schema-Datei (PRUEM DNA.xsd) festgelegt.

4.2.1. Schema PRUEMDNAx

Das Schema enthält folgende Felder:

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

4.2.2. Inhalt der Header-Strukur

4.2.2.1. PRUEM Header

Diese Struktur beschreibt den Header der XML-Datei. Sie enthält folgende Felder:

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

4.2.2.2. PRUEM_header dir

In der Nachricht enthaltene Datentypen; folgende Werte sind möglich:

Value	Description
R	Request

Value	Description
A	Answer

4.2.2.3. PRUEM header info

Struktur zur Beschreibung des Mitgliedstaats sowie des Datums/Zeitpunkts der Nachricht. Sie umfasst folgende Felder:

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

4.2.3. Inhalt der PRUEM-Datenprofile

4.2.3.1. PRUEM_datas

Diese Struktur beschreibt den XML-Datenbereich des Profils. Sie enthält folgende Felder:

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

4.2.3.2. PRUEM_request_type

In der Nachricht enthaltene Datentypen; folgende Werte sind möglich:

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

4.2.3.3. PRUEM_hitquality_type

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

4.2.3.4. PRUEM_data_type

In der Nachricht enthaltene Datentypen; folgende Werte sind möglich:

Value	Description
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

In der Nachricht enthaltene Datentypen; folgende Werte sind möglich:

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

4.2.3.6. IPSG_DNA_profile

Struktur zur Beschreibung eines DNA-Profils. Sie enthält folgende Felder:

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

4.2.3.7. IPSG_DNA_ISSOL

Struktur, welche die ISSOL-Loci (Standard Group of Interpol loci) angibt. Sie enthält folgende Felder:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

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

4.2.3.8. IPSG_DNA_additional_loci

Struktur, welche die weiteren Loci enthält. Sie umfasst folgende Felder:

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

4.2.3.9. IPSG_DNA_locus

Struktur, die einen Locus beschreibt. Sie enthält folgende Felder:

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

5. *Anwendungs-, Sicherheits und Kommunikationsarchitektur*

5.1. *Überblick*

Zur Implementierung der Anwendungen für den DNA-Datenaustausch im Rahmen des Beschlusses 2008/615/JI sollte ein gemeinsames logisch abgeschlossenes Telekommunikationsnetz zwischen den Mitgliedstaaten genutzt werden. Um eine effizientere Nutzung dieser gemeinsamen Kommunikationsinfrastruktur für die Übermittlung

der Anfragen sowie der eintreffenden Antworten zu gewährleisten, wird ein asynchroner Mechanismus zur Verschlüsselung der in SMTP E-Mail-Nachrichten verpackten Anfragen zu DNA-Daten und daktyloskopischen Daten festgelegt. Zur Erfüllung der Sicherheitsanforderungen wird s/MIME als Erweiterung der SMTP-Funktionalität genutzt, um einen echten End-zu-End-Tunnel über das Netz einzurichten.

Das operative TESTA-Netzwerk (Trans European Services for Telematics between Administrations) wird als Kommunikationsnetz für den Datenaustausch zwischen den Mitgliedstaaten genutzt. TESTA fällt in den Verantwortungsbereich der Europäischen Kommission. In Anbetracht dessen, dass sich die nationalen DNA-Datenbanken und die derzeitigen nationalen TESTA-Zugangspunkte an unterschiedlichen Orten in den Mitgliedstaaten befinden können, kann ein Zugang zu TESTA hergestellt werden entweder

1. durch Nutzung des bestehenden nationalen Zugangspunktes oder durch Einrichtung eines neuen nationalen TESTA-Zugangspunktes oder

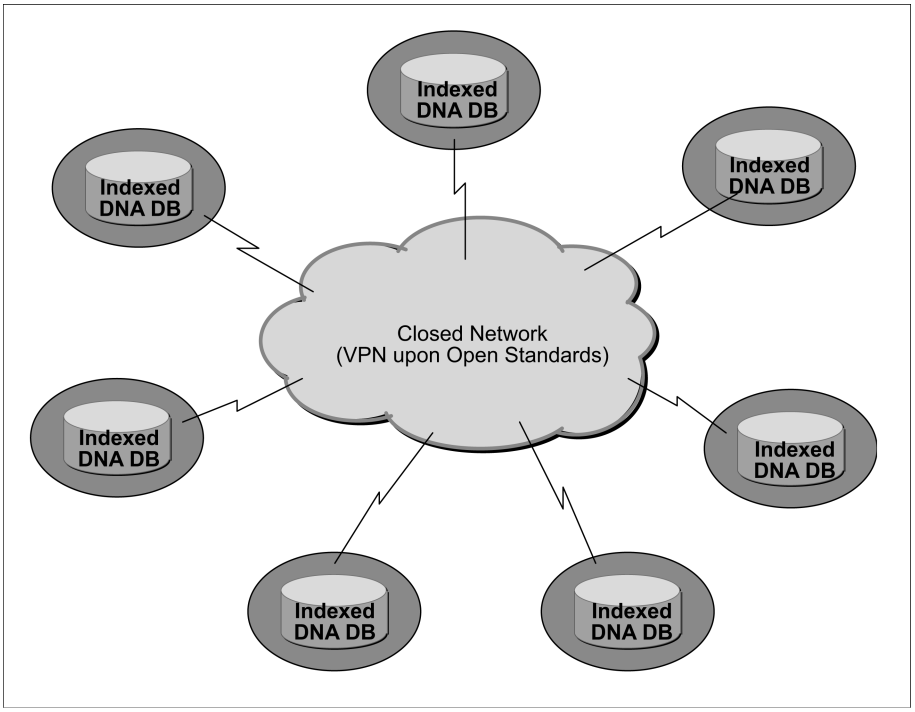
2. durch Einrichtung einer gesicherten lokalen Verbindung zwischen dem Ort, an dem sich die DNA-Datenbank befindet und von der zuständigen nationalen Behörde verwaltet wird, und dem bestehenden nationalen TESTA-Zugangspunkt.

Die laut Durchführungsbeschluss 2008/615/JI anzuwendenden Protokolle und Normen beruhen auf offenen Standards und erfüllen die Auflagen der Entscheidungsträger für die nationale Sicherheitspolitik in den Mitgliedstaaten.

5.2. *Höhere Architekturebenen*

Gemäß dem Beschluss 2008/615/JI stellt jeder Mitgliedstaat seine DNA-Daten für den Austausch mit und/oder den Abruf durch andere Mitgliedstaaten im allgemeinen Standarddatenformat zur Verfügung. Die Architektur basiert auf einem „any-to-any"-Kommunikationsmodell. Es gibt weder einen Zentralserver noch eine zentralisierte Datenbank zur Speicherung der DNA-Profile.

Abbildung 1: Topologie des DNA-Datenaustauschs



Zusätzlich zur Erfüllung nationaler rechtlicher Auflagen der Mitgliedstaaten kann jeder Mitgliedstaat entscheiden, welche Art von Hardware und Software bei der Konfiguration seines Standorts eingesetzt werden sollte, um den Anforderungen des Beschlusses 2008/615/JI gerecht zu werden.

5.3. *Sicherheitsstandards und Datenschutz*

Drei Ebenen von Sicherheitsaspekten wurden geprüft und umgesetzt.

5.3.1. Datenebene

Die von den einzelnen Mitgliedstaaten bereitgestellten DNA-Profildaten müssen mit einem gemeinsamen Datenschutzstandard übereinstimmen, so dass der anfragende Mitgliedstaat eine Information hauptsächlich über Übereinstimmung oder Nichtübereinstimmung (HIT oder No-HIT) erhält, wobei im Trefferfall (HIT) zugleich eine Identifizierungsnummer ohne personenbezogene Daten übermittelt wird. Die weiteren Ermittlungen nach einer Treffermeldung werden auf bilateraler Ebene entsprechend den nationalen rechtlichen und organisatorischen Vorschriften, denen die nationalen Standorte der betreffenden Mitgliedstaaten unterliegen, geführt.

5.3.2. Kommunikationsebene

Nachrichten mit DNA-Profil-Informationen (Anfragen und Antworten) werden anhand eines dem Stand der Technik entsprechenden Mechanismus, der offenen Standards wie beispielsweise s/MIME entspricht, verschlüsselt, bevor sie an die betreffenden Stellen der anderen Mitgliedstaaten übermittelt werden.

5.3.3. Übermittlungsebene

Alle verschlüsselten Nachrichten, die DNA-Profil-Informationen enthalten, werden den Standorten der anderen Mitgliedstaaten über ein VPN-(virtuelles privates Netzwerk)-Tunnelsystem zugeleitet, das auf internationaler Ebene von einem vertrauenswürdigen Netzbetreiber verwaltet wird; für die Einrichtung einer sicheren Verbindung zu diesem Tunnelsystem sind die einzelnen Mitgliedstaaten zuständig. Dieses VPN-Tunnelsystem hat keinen Verbindungspunkt mit dem offenen Internet.

5.4. *Für den Verschlüsselungsmechanismus zu verwendende Protokolle und Standards: s/MIME und dazugehörige Softwarepakete*

Zur Verschlüsselung von Nachrichten mit DNA-Profil-Informationen wird der offene Standard s/MIME, der den „de facto"-E-Mailstandard SMTP ergänzt, verwendet. Das Protokoll s/MIME (V3) unterstützt signierte Empfangsbestätigungen, Sicherheitsmarke (Security Label) und gesicherte Mailinglisten und basiert auf der Cryptographic Message Syntax (CMS), einer IETF-Spezifikation für kryptografisch geschützte Nachrichten. Es kann zur digitalen Signatur, Prüfsummenerstellung, Authentifizierung oder Verschlüsselung von digitalen Daten jeglicher Form verwendet werden.

Das für den s/MIME-Mechanismus verwendete Zertifikat muss dem Standard X.509 entsprechen. Um einheitliche Standards und Verfahren mit anderen Prümer Anwendungen sicherzustellen, gelten für s/MIME-Verschlüsselungsvorgänge oder zur Verwendung unterschiedlicher kommerzieller Standardprodukte (COTS — Commercial Product of the Shelves) folgende Bearbeitungsregeln:

— Die Reihenfolge der Arbeitsvorgänge ist: erst verschlüsseln, dann signieren.

— Die Verschlüsselungsalgorithmen AES (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit und RSA mit einer Schlüssellänge von 1 024 Bit werden jeweils für die symmetrische und die asymmetrische Verschlüsselung verwendet.

— Der Hash-Algorithmus SHA-1 wird benutzt.

Die s/MIME-Funktionalität ist bereits Bestandteil der überwiegenden Mehrzahl moderner E-Mail-Softwarepakete einschließlich Outlook, Mozilla Mail sowie Netscape Communicator 4.x und bietet eine Interoperabilität mit allen gängigen E-Mail-Softwarepaketen.

Aufgrund der einfachen Integration von s/MIME in die nationale IT-Infrastruktur an allen Standorten der Mitgliedstaaten wurde es als funktionsfähiger Mechanismus zur Realisierung der Sicherheitsstufe der Kommunikation ausgewählt. Um das Ziel „Konzeptnachweis (Proof of Concept)" effizienter zu erreichen und Kosten zu senken, wurde jedoch der offene Standard Java Mail API für den Prototyp des DNA-Datenaustauschs gewählt. JavaMail API ermöglicht eine einfache Ver- und Entschlüsselung von E-Mails unter Einsatz von s/MIME und/oder OpenPGP. Es ist beabsichtigt, eine einzelne, leicht zu nutzende Schnittstelle für E-Mail-Clients bereitzustellen, die verschlüsselte E-Mails in den beiden geläufigsten E-Mail-Verschlüsselungsformaten verschicken und erhalten sollen. Daher genügen alle dem Stand der Technik entsprechenden Implementierungen der JavaMail-API den Anforderungen gemäß dem Beschluss 2008/615/JI, beispielsweise das Produkt Bouncy Castle JCE (Java Cryptographic Extension), das genutzt wird, um s/MIME für den Prototyp des DNA-Datenaustauschs zwischen allen Mitgliedstaaten zu implementieren.

5.5. *Anwendungsarchitektur*

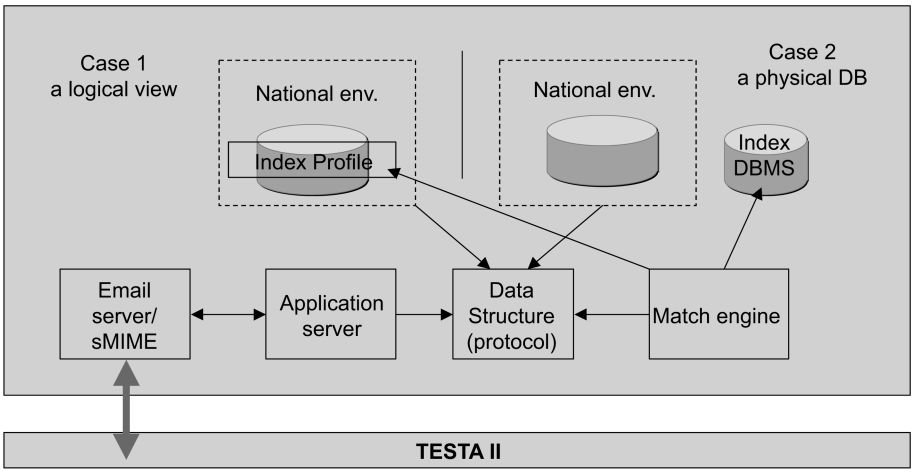
Jeder Mitgliedstaat stellt jedem anderen Mitgliedstaat einen Satz (Set) standardisierter DNA-Profildaten zur Verfügung, die dem aktuellen gemeinsamen ICD entsprechen. Dies kann entweder durch Bereitstellung einer logischen Sicht (logical view) der eigenen nationalen Datenbank erfolgen, oder aber durch Einrichtung einer physisch exportierten Datenbank (Indexdatenbank).

Anhand der vier Hauptkomponenten — E-Mail Server/s/MIME, Anwendungsserver, Data Structure Area für den Abruf/die Eingabe von Daten und zur Registrierung der eingehenden/ausgehenden Nachrichten, sowie Match Engine — wird die gesamte Anwendungslogik anbieterunabhängig implementiert.

Um allen Mitgliedstaaten eine unkomplizierte Integration der Komponente in ihre jeweiligen nationalen Standorte zu ermöglichen, wurde die festgelegte gemeinsame Funktionalität anhand von Open-Source-Komponenten implementiert, die von den einzelnen Mitgliedstaaten entsprechend ihrer jeweiligen nationalen IT-Politik und ihren Vorschriften ausgewählt werden können. Aufgrund der anbieterunabhängigen Merkmale, die zu implementieren sind, um Zugang zu den Indexdatenbanken mit den DNA-Profilen zu erhalten, die in den Anwendungsbereich des Beschlusses 2008/615/JI fallen, genießt jeder Mitgliedstaat Entscheidungsfreiheit bei der Wahl seiner Hardware und Software-Plattform, einschließlich der Datenbank- und Betriebssysteme.

Für den DNA-Datenaustausch wurde ein Prototyp entwickelt und auf dem bestehenden gemeinsamen Netzwerk mit Erfolg getestet. Die Version 1.0 wurde in die Produktionsumgebung eingebunden und befindet sich im täglichen operativen Einsatz. Die Mitgliedstaaten können dieses gemeinsam entwickelte Produkt nutzen oder aber ihre eigenen Produkte entwickeln. Die gemeinsamen Produktkomponenten werden gewartet, bedarfsgerecht angepasst und entsprechend den im Wandel befindlichen informationstechnischen, forensischen bzw. polizeifachlichen Anforderungen weiterentwickelt.

Abbildung 2: Überblick über die Anwendungstopologie



5.6. *Für die Anwendungsarchitektur zu verwendende Protokolle und Standards*

5.6.1. XML

Für den DNA-Datenaustausch wird in vollem Umfang das XML-Schema verwendet, das den SMTP-E-Mail-Nachrichten als Attachment beigefügt wird. XML (eXtensible Markup Language) ist eine vom W3C empfohlene allgemeine Markup-Sprache (Bezeichnungssprache) zur Schaffung spezieller Markup-Sprachen, mit denen viele verschiedene Arten von Daten beschrieben werden können. Das für den Austausch zwischen allen Mitgliedstaaten geeignete DNA-Profil wird im ICD-Dokument anhand von XML und dem XML-Schema beschrieben.

5.6.2. ODBC

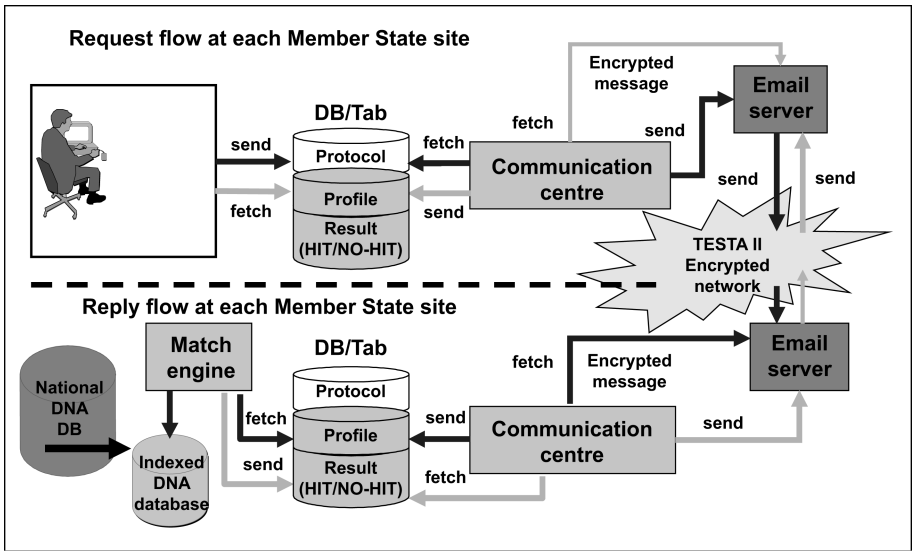
Open DataBase Connectivity (ODBC) ist eine auf Standardsoftware gestützte API-Methode für den Zugang zu Datenbankverwaltungssystemen und macht sie unabhängig von Programmiersprachen, Datenbanken und Betriebssystemen. Allerdings hat ODBC auch einige Nachteile. Die Verwaltung einer großen Anzahl von Client-Maschinen kann dazu führen, dass eine Vielzahl von Treibern (Drivers) und DLL einbezogen werden. Diese Komplexität kann den mit der Systemverwaltung verbundenen Aufwand erhöhen.

5.6.3. JDBC

Java DataBase Connectivity (JDBC) ist ein API für die Programmiersprache Java, die definiert, auf welche Weise ein Client Zugang zu einer Datenbank erhält. Im Gegensatz zu ODBC erfordert JDBC nicht die Verwendung eines bestimmten Satzes von lokalen DLL im Desktop.

Die Geschäftslogik zur Bearbeitung von DNA-Profil-Anfragen und -Antworten an jedem Standort der Mitgliedstaaten veranschaulicht die folgende Zeichnung. Sowohl die bei einer Anfrage als auch bei einer Antwort generierten Datenflüsse interagieren mit einem neutralen Datenbereich, der unterschiedliche Datenpools mit einer gemeinsamen Datenstruktur umfasst.

Abbildung 3: Übersicht über den Anwendungs-Workflow im Standort der einzelnen Mitgliedstaaten



5.7. *Kommunikationsumgebung*

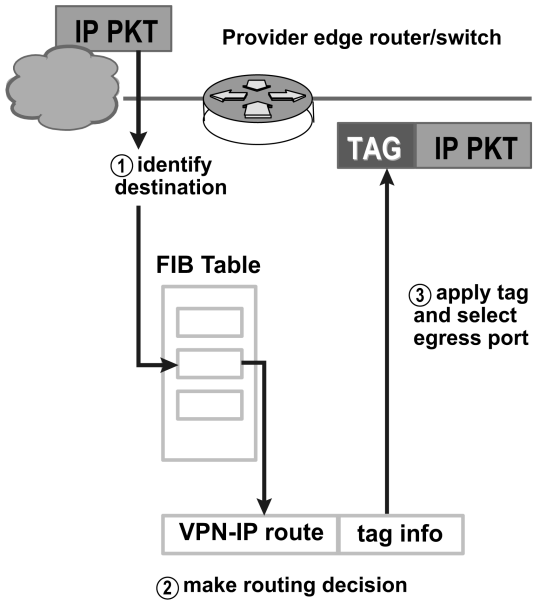
5.7.1. Gemeinsames Kommunikationsnetzwerk: TESTA und seine Nachfolgeinfrastruktur

Für den DNA-Austausch nutzte die Anwendung E-Mails — ein asynchroner Mechanismus — zur Übermittlung von Anfragen und zur Entgegennahme von Antworten zwischen den Mitgliedstaaten. Da alle Mitgliedstaaten zumindest einen nationalen Zugangspunkt zu dem TESTA-Netzwerk haben, wird dieses für den DNA-Datenaustausch genutzt. TESTA bietet mit seinem E-Mail-Relay eine Reihe von Mehrwertdiensten. Neben dem Hosting TESTA-spezifischer E-Mail-Boxen ist die Infrastruktur in der Lage, Mailing-Verteilerlisten und Routing-Regelungen (Routing Policies) zu implementieren. Damit kann TESTA als Clearingstelle für Nachrichten eingesetzt werden, die an Behörden innerhalb der EU-weiten Domäne adressiert sind. Es können auch Virenprüffunktionen eingerichtet werden.

Das durch eine Firewall geschützte TESTA E-Mail-Relay ist auf einer Hardware-Plattform mit hoher Verfügbarkeit aufgebaut, die sich im zentralen Standort der TESTA-Anwendung befindet. Die Domänennamendienste DNS (Domain Name Services) lösen Namensbezeichnungen (Resource Locators) in IP-Adressen auf und verstecken Adressierungen vor den Benutzern oder Anwendungen.

5.7.2. Sicherheitserwägungen

Im TESTA-Umfeld wurde das Konzept eines VPN (virtuelles privates Netzwerk) umgesetzt. Die für den Aufbau dieses VPN verwendete Tag-Switching-Technologie wird weiterentwickelt werden, um den IETF-Standard (Internet Engineering Task Force) MPLS (Multi-Protocol Label Switching) zu unterstützen.



MPLS ist eine auf dem IETF-Standard basierende Technologie, die den Datenfluss im Netzwerk durch Vermeidung der Paketanalyse durch Zwischen-Router („Hops") beschleunigt. Dies erfolgt auf der Grundlage so genannter Labels (Kennsätze), die durch Edge-Router des Backbones an das Datenpaket angehängt werden, auf der Basis der Informationen, die in der FIB (Forwarding Information Base) gespeichert sind. Labels werden auch zur Einrichtung virtueller privater Netze (VPNs) verwendet.

MPLS kombiniert die Vorteile des Layer-3-Routing mit denen des Layer-2-Switching. Da IP-Adressen beim Durchlaufen des Backbones nicht evaluiert werden, werden von MPLS keine Beschränkungen für IP-Adressierung auferlegt.

Darüber hinaus werden E-Mails im TESTA-Netzwerk durch einen s/MIME-gesteuerten Verschlüsselungsmechanismus geschützt. Ohne Schlüssel und das erforderliche Zertifikat können verschlüsselte Nachrichten in diesem Netzwerk nicht entschlüsselt werden.

5.7.3. Für das Kommunikationsnetzwerk zu verwendende Protokolle und Standards

5.7.3.1. SMTP

Das SMTP-Protokoll (Simple Mail Transfer Protocol) ist De-Facto-Standard für die Übermittlung von E-Mails über das Internet. SMTP ist ein relativ einfaches, textbasiertes Protokoll, bei dem ein oder mehrere Empfänger einer Nachricht angegeben werden, woraufhin der Text der Nachricht übermittelt wird. SMTP verwendet den TCP-Port 25 entsprechend der IETF-Spezifikation. Zur Bestimmung des SMTP-Servers für einen bestimmten Domänennamen wird der MX-(Mail eXchange)-DNS-(Domain Name Systems)-Record verwendet.

Da dieses Protokoll ursprünglich ausschließlich ASCII-textbasiert war, gab es Schwierigkeiten mit binären Dateien. Zur Aufbereitung binärer Dateien im Hinblick auf ihre Übermittlung durch SMTP wurden Standards wie MIME ausgearbeitet. Gegenwärtig unterstützen die meisten SMTP-Server die 8BITMIME- und s/MIME-Erweiterungen, so dass binäre Dateien fast ebenso einfach wie „Nur Text" (plain text) übermittelt werden können. Die Arbeitsabläufe für s/MIME-Operationen werden im Abschnitt über s/MIME (siehe Kapitel 5.4) beschrieben.

SMTP ist ein „Push"-Protokoll, d. h., es bietet nicht die Möglichkeit, auf Verlangen von einem Remote-Server Nachrichten abzurufen („pull"). Um dies zu ermöglichen, muss der Mail-Client POP3 oder IMAP benutzen. Es wurde beschlossen, zur Implementierung des DNA-Datenaustauschs das Protokoll POP3 zu verwenden.

5.7.3.2. POP

Lokale E-Mail-Clients verwenden die Version 3 des Post Office Protocol (POP3), ein Internet-Standardprotokoll (der Anwendungsschicht), zum Abruf einer E-Mail von einem Remote-Server übe eine TCP/IP-Verbindung. Unter Verwendung des SMTP-Submit-Profils des SMTP-Protokolls können E-Mail-Clients Nachrichten über das Internet oder interne Firmennetze übermitteln. MIME bildet den Standard für Attachments und Nicht-ASCII-Texte bei der Übermittlung von E-Mails. Obgleich weder POP3 noch SMTP MIME-formatierte E-Mails benötigen, erfolgt der E-Mail-Verkehr im Internet im Wesentlichen MIME-formatiert, so dass POP-Clients in der Lage sein müssen, MIME zu verstehen und anzuwenden. Die gesamte Kommunikationsumgebung nach Beschluss 2008/615/JI wird daher die Komponenten des POP integrieren.

5.7.4. Zuweisung der Netzwerkadressen

Operative Umgebung

Die europäische IP-Registrierungsbehörde RIPE hat TESTA unlängst einen speziellen Subnet-Adressenblock der Klasse C zugewiesen. Erforderlichenfalls können TESTA künftig weitere Adressenblocks zugewiesen werden. Die Zuordnung von IP-Adressen an die Mitgliedstaaten erfolgt im Allgemeinen nach einem geografischen Schema in Europa. Der Datenaustausch zwischen Mitgliedstaaten im Rahmen des Beschlusses 2008/615/JI erfolgt im Wege eines EU-weiten logisch geschlossenen IP-Netzwerks.

Testumgebung

Damit allen angeschlossenen Mitgliedstaaten eine reibungslos funktionierende Operationsumgebung geboten werden kann, ist es erforderlich, für neue Mitgliedstaaten, die ihre Teilnahme an dem Datenaustausch vorbereiten, eine auf dem geschlossenen Netzwerk aufbauende Testumgebung zu schaffen. Es wurde eine Vorlage mit Parametern, darunter IP-Adressen, Netzeinstellungen, E-Mail-Domänen sowie Benutzerkonten, festgelegt, die in den betreffenden Standorten der Mitgliedstaaten eingerichtet werden sollten. Zudem wurde für Testzwecke ein Satz von „Pseudo"-DNA-Profilen erstellt.

5.7.5. Konfigurationsparameter

Es wurde ein sicheres E-Mail-System auf der Grundlage der Domäne eu-admin.net eingerichtet. Diese Domäne und die assoziierten Adressen sind vor einem Zugriff durch Stellen außerhalb der EU-weiten TESTA-Domäne geschützt, da die betreffenden Namen nur dem zentralen DNS-Server von TESTA bekannt sind, der vom Internet abgeschirmt ist.

Die Zuordnung (Mapping) dieser TESTA-Site-Adressen („host names") zu den IP-Adressen wird vom TESTA-DNS-Dienst vorgenommen. Für jede lokale Domäne wird ein Mail-Eintrag in diesen zentralen DNS-Server von TESTA eingefügt, so dass alle an die lokalen TESTA-Domänen geschickten E-Mail-Nachrichten dem zentralen Mail-Relay von TESTA zugeleitet werden. Dieses zentrale Mail-Relay leitet sie dann anhand der E-Mail-Adressen der lokalen Domäne an den speziellen E-Mail-Server der lokalen Domäne weiter. Durch dieses Verfahren zur Übermittlung von E-Mails durchlaufen vertrauliche Informationen ausschließlich die EU-weite geschlossene Netzwerkinfrastruktur und nicht das unsichere Internet.

In allen Standorten der Mitgliedstaaten ist es erforderlich, Subdomänen (***Fett- und Kursivdruck***) einzurichten, die der folgenden Syntax entsprechen:

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

„***Member State-code***" den Wert des aus 2 Buchstaben zusammengesetzten Mitgliedstaatencodes annimmt (z. B. AT, BE usw.) und

„***application-type***" einen der folgenden Werte annimmt: DNA und FP.

In Anwendung der oben genannten Syntax erhalten die Subdomänen der Mitgliedstaaten folgende Form:

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

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

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

KAPITEL 2: **Austausch daktyloskopischer Daten (Schnittstellenkontrolldokument)**

Mit dem folgenden Schnittstellenkontrolldokument sollen die Anforderungen für den Austausch daktyloskopischer Daten zwischen den Automatisierten Fingerabdruck-Identifizierungs-Systemen (AFIS) der Mitgliedstaaten festgelegt werden. Es stützt sich auf die Interpol-Implementierung des ANSI/NIST-ITL 1-2000-Standards (INT-I, Version 4.22b).

In dieser Fassung werden alle grundlegenden Definitionen für Datensätze der Typen Typ 1, Typ 2, Typ 4, Typ 9, Typ 13 und Typ 15 erfasst, die für eine Fingerabdruckverarbeitung erforderlich sind, die sich auf Bilder und Minutien stützt.

1. ***Übersicht über den Dateiinhalt***

Eine Fingerabdruckdatei besteht aus verschiedenen logischen Datensätzen. Im ursprünglichen ANSI/NIST-ITL 1-2000-Standard gibt es 16 Typen von Datensätzen. Zwischen den Datensätzen und zwischen den Feldern und Unterfeldern innerhalb der Datensätze werden geeignete ASCII-Trennzeichen verwendet.

Nur 6 Datensatz-Typen werden für den Informationsaustausch zwischen der Sendestelle und der Empfangsstelle verwendet:

Typ 1	->	Transaktionsinformationen
Typ 2	->	Alphanumerische Personen-/Falldaten
Typ 4	->	Hochauflösende Fingerabdruckbilder in Grautönen
Typ 9	->	Minutiendatensätze
Typ 13	->	Datensatz mit Bildern von Fingerabdruck- und Handflächenabdruckspuren in variabler Auflösung
Typ 15	->	Datensatz mit Bildern von Handflächenabdrücken in variabler Auflösung

1.1. *Typ 1 — File Header*

Dieser Datensatz enthält Routing-Informationen und Informationen zur Beschreibung der Struktur der übrigen Datei. In dieser Datensatzart werden ferner die Transaktionstypen definiert, die unter die folgenden Kategorien fallen:

1.2. *Typ 2 — Descriptive Text*

Dieser Datensatz enthält Textinformationen, die für die Sende- und die Empfangsstellen von Interesse sind.

1.3. *Typ 4 — High Resolution Gray-scale Image*

Dieser Datensatz dient zum Austausch hochauflösender Fingerabdruckbilder (500 Pixel/Inch) in Graustufen (8 Bit). Die Fingerabdruckbilder werden mit dem WSQ-Algorithmus in einem Verhältnis von nicht mehr als 15:1 komprimiert. Andere Algorithmen für die Komprimierung oder nichtkomprimierte Bilder dürfen nicht verwendet werden.

1.4. *Typ 9 — Minutiæ Record*

Typ-9-Datensätze dienen zum Austausch von Merkmalen der Papillarlinien oder Minutien. Mit diesen Datensätzen wird zum einen bezweckt, eine unnötige Doppelung von AFIS-Kodierungsprozessen zu vermeiden, und zum anderen, die Übertragung von AFIS-Codes, die weniger Daten enthalten als die entsprechenden Bilder, zu ermöglichen.

1.5. *Typ 13 — Variable-Resolution Latent Image Record*

Diese Datensätze werden verwendet, um Fingerabdruckspuren und Handflächenabdruckspuren in variabler Auflösung zusammen mit alphanumerischen Textinformationen zu übermitteln. Die Scan-Auflösung der Bilder beträgt 500 Pixel/Inch mit 256 Graustufen. Wenn die Qualität des Spurenbildes dafür ausreicht, wird es mit einem WSQ-Algorithmus komprimiert. Erforderlichenfalls kann die Bildauflösung durch bilaterale Vereinbarung auf mehr als 500 Pixel/Inch und mehr als 256 Graustufen ausgeweitet werden. Für diesen Fall wird dringend empfohlen, JPEG-2000 zu verwenden (siehe Anlage 7).

1.6. *Typ 15 — Variable-Resolution Palmprint Image Record*

Datensätze mit nummerierten Feldern werden verwendet, um Handabdruckbilder in variabler Auflösung zusammen mit alphanumerischen Textinformationen auszutauschen. Die Scan-Auflösung der Bilder beträgt 500 Pixel/Inch mit 256 Graustufen. Für ein möglichst geringes Datenaufkommen werden alle Handabdruckbilder mit einem WSQ-Algorithmus komprimiert. Erforderlichenfalls kann die Bildauflösung durch bilaterale Vereinbarung auf mehr als 500 Pixel/Inch und mehr als 256 Graustufen ausgeweitet werden. Für diesen Fall wird dringend empfohlen, JPEG-2000 zu verwenden (siehe Anlage 7).

2. ***Datensatz-Format***

Eine Transaktionsdatei besteht aus einem oder mehreren logischen Datensätzen. Für jeden Datensatz in der Datei müssen mehrere für den Datensatztyp geeignete Informationsfelder vorhanden sein. Jedes Informationsfeld kann ein oder mehrere grundlegende Informationselemente mit einheitlichem Wert enthalten. Zusammen werden diese Elemente verwendet, um unterschiedliche Aspekte der in dem Feld enthaltenen Daten deutlich zu machen. Ein Informationsfeld kann auch aus einem oder mehreren Informationselementen bestehen, die zusammengruppiert und innerhalb eines Felds mehrfach wiederholt werden. Eine solche Gruppe von Informationselementen ist als Unterfeld bekannt. Ein Informationsfeld kann somit aus einem oder mehreren Unterfeldern mit Informationselementen bestehen.

2.1. *Informationstrennzeichen (Information Separators)*

In den Datensätzen mit nummerierten Feldern wird die Abgrenzung der Informationen durch 4 ASCII-Informationstrennzeichen erreicht. Bei den voneinander abgegrenzten Informationen kann es sich um Elemente innerhalb eines Felds oder Unterfelds, um Felder innerhalb eines Datensatzes oder um mehrfach vorkommende Unterfelder handeln. Diese Informationstrennzeichen sind im ANSI-Standard X3.4 definiert. Die Zeichen werden verwendet, um Informationen logisch voneinander abzugrenzen und festzulegen. In einem hierarchischen Bezug betrachtet ist das Dateitrennzeichen „FS“ (File Separator) das umfassendste Trennzeichen, gefolgt vom Gruppentrennzeichen „GS“ (Group Separator), dem Datensatztrennzeichen „RS“ (Record Separator) und schließlich dem Einheitentrennzeichen „US“ (Unit Separator). In Tabelle 1 sind diese ASCII-Trennzeichen und eine Beschreibung ihrer Verwendung in dem vorliegenden Standard enthalten.

Informationstrennzeichen sind ihrer Funktion nach als Angabe der darauf folgenden Datenart zu sehen. Das Zeichen „US“ grenzt einzelne Informationselemente innerhalb eines Felds oder Unterfelds voneinander ab. Es zeigt an, dass das nächste Informationselement Bestandteil der Daten dieses Felds oder Unterfelds ist. Bei mehrfachen Unterfeldern innerhalb eines Felds, die durch das Zeichen „RS“ voneinander abgegrenzt werden, wird mit dem Zeichen der Beginn der nächsten Gruppe sich wiederholender Informationselemente angezeigt. Das Trennzeichen „GS“, das zwischen Informationsfeldern verwendet wird, zeigt den Beginn eines neuen Felds vor der Feldidentifizierungsnummer an, die erscheinen soll. Auf die gleiche Weise wird der Beginn eines neuen Datensatzes durch das Trennzeichen „FS“ angezeigt.

Die 4 Zeichen haben nur eine Bedeutung, wenn sie als Trennzeichen für Datenelemente in den Feldern der ASCII-Textrecords verwendet werden. Die Trennzeichen haben in binären Bilddatensätzen und binären Feldern keine besondere Bedeutung, sie gehören lediglich zu den ausgetauschten Daten.

Normalerweise sollte es keine leeren Felder oder Informationselemente geben, daher sollte zwischen allen Datenelementen lediglich ein Trennzeichen stehen. Die Ausnahme von dieser Regel liegt vor, wenn die Daten in Feldern oder Informationselemente in einer Transaktion nicht verfügbar sind, fehlen oder fakultativ sind und die Transaktion nicht davon abhängt, ob diese spezifischen Daten vorhanden sind. In diesen Fällen erscheinen mehrfache und nebeneinander liegende Trennzeichen zusammen; es ist nicht erforderlich, zwischen den Trennzeichen fiktive Daten einzufügen.

Für die Definition eines Felds, das aus 3 Informationselementen besteht, gilt Folgendes. Fehlt die Information für das zweite Informationselement, so würden 2 nebeneinander stehende Informationstrennzeichen „US“ zwischen dem ersten und dem dritten Informationselement erscheinen. Würde sowohl das zweite als auch das dritte Informationselement fehlen, so sollten 3 Trennzeichen verwendet werden, nämlich 2 „US“-Trennzeichen zusätzlich zu dem abschließenden Trennzeichen für das Feld oder Unterfeld. Allgemein lässt sich sagen, dass die entsprechende Zahl von Trennzeichen eingefügt werden sollte, wenn ein oder mehr obligatorische oder fakultative Informationselemente für ein Feld oder Unterfeld nicht vorhanden sind.

Es können 2 oder mehr der 4 zur Verfügung stehenden Trennzeichen nebeneinander kombiniert werden. Wenn Daten für Informationselemente, Unterfelder oder Felder fehlen oder nicht zur Verfügung stehen, muss es ein Trennzeichen weniger geben als die erforderliche Zahl der Datenelemente, Unterfelder oder Felder.

Tabelle 1: Verwendete Trennzeichen

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. *Datensatzlayout*

Bei Datensätzen mit nummerierten Feldern muss jedes verwendete Informationsfeld gemäß diesem Standard nummeriert werden. Das Format für jedes Feld muss aus der Nummer des Datensatztyps, gefolgt von einem Punkt „.“, einer Feldnummer gefolgt von einem Doppelpunkt „:“, gefolgt von der dem Feld entsprechenden Information bestehen. Die Feldnummer kann aus einer Zahl mit den Ziffern 1 bis 9 zwischen dem Punkt „.“ und dem Doppelpunkt „:“ bestehen. Die Feldnummer ist als vorzeichenloser Ganzzahlenwert zu betrachten. Dies bedeutet, dass die Feldnummer „2.123:“ der Feldnummer „2.000000123:“ entspricht und in der gleichen Weise ausgelegt werden sollte.

Zu Illustrationszwecken in diesem Dokument wird eine 3-stellige Zahl für die Felder verwendet, die in jedem der beschriebenen nummerierten Datensätze enthalten sind. Feldnummern haben die Form „TT.xxx:“, wobei „TT“ für den Datensatztyp mit 1 oder 2 Zeichen steht, gefolgt von einem Punkt. Die nächsten 3 Zeichen enthalten die entsprechende Feldnummer, gefolgt von einem Doppelpunkt. Die beschreibenden ASCII-Informationen oder die Bilddaten folgen auf den Doppelpunkt.

Die logischen Typ-1- und Typ-2-Datensätze enthalten nur ASCII-Textdatenfelder. Die gesamte Länge des Datensatzes (einschließlich Feldnummern, Doppelpunkten und Trennzeichen) wird als erstes ASCII-Feld innerhalb dieser Datensatztypen verzeichnet. Das Kontrollzeichen des ASCII-Dateitrennzeichens „FS“ (das das Ende des Datensatzes oder der Transaktion bezeichnet) folgt auf das letzte Byte der ASCII-Information und wird in die Länge des Datensatzes mit einbezogen.

Im Gegensatz zum Konzept der nummerierten Felder enthält der Typ-4-Datensatz ausschließlich binäre Daten, die als geordnete binäre Felder mit fester Länge verzeichnet werden. Die gesamte Länge des Datensatzes wird im ersten binären Feld mit 4 Bytes eines jeden Datensatzes verzeichnet. Bei diesem binären Datensatz wird weder die Datensatznummer mit dem Punkt noch die Feldnummer und der darauf folgende Doppelpunkt verzeichnet. Darüber hinaus werden die 4 Trennzeichen („US“, „RS“, „GS“ oder „FS“) ausschließlich als binäre Daten interpretiert, da alle Feldlängen dieses Datensatzes entweder festgelegt oder spezifiziert sind. Das Trennzeichen „FS“ darf bei dem binären Datensatz nicht als Datensatztrennzeichen oder Zeichen für das Transaktionsende verwendet werden.

3. ***Typ-1-Datensatz: File Header***

Dieser Datensatz beschreibt die Dateistruktur, den Dateityp und andere wichtige Informationen. Der Zeichensatz für Typ-1-Felder darf nur den 7-Bit-ANSI-Code für den Informationsaustausch enthalten.

3.1. *Felder für Typ-1 logischer Datensatz*

3.1.1. Feld 1.001: Logical Record Length (LEN)

Dieses Feld enthält die Gesamtzahl der Bytes im gesamten Typ-1 logischen Datensatz. Das Feld beginnt mit „1.001:“, gefolgt von der Gesamtlänge des Datensatzes einschließlich der Zeichen in jedem Feld inklusive der Trennzeichen.

3.1.2. Feld 1.002: Version Number (VER)

Um sicherzustellen, dass die Nutzer wissen, welche Version des ANSI/NIST-Standards verwendet wird, ist in diesem Feld mit 4 Bytes die Versionsnummer des Standards angegeben, die von der Software oder dem System, das die Datei anlegt, benutzt wird. Die ersten beiden Bytes geben die führenden Stellen der Versionsnummer an, die zweiten beiden Bytes die Revisionsnummer. Beispielsweise würde der ursprüngliche Standard von 1986 als die erste Version betrachtet und „0100" genannt, während der gegenwärtige ANSI/NIST-ITL 1-2000-Standard „0300" genannt wird.

3.1.3. Feld 1.003: File Content (CNT)

In diesem Feld ist jeder der Datensätze in der Datei nach Datensatztyp und der Reihenfolge aufgeführt, in der die Datensätze in der Datei erscheinen. Es besteht aus einem oder mehreren Unterfeldern, von denen jedes wiederum 2 Informationselemente enthält, die einen einzelnen Datensatz beschreiben, der sich in der vorliegenden Datei befindet. Die Unterfelder werden in der gleichen Reihenfolge angegeben, in der die Datensätze gespeichert und übertragen werden.

Das erste Informationselement im ersten Unterfeld ist „1"; damit wird Bezug auf diesen Typ-1-Datensatz genommen. Darauf folgt ein zweites Informationselement, das die Anzahl aller Datensätze in der Datei enthält. Diese Zahl ist gleich der Anzahl der Unterfelder von Feld 1.003.

Jedes der Unterfelder gehört zu einem Datensatz innerhalb der Datei, und die Reihenfolge der Unterfelder entspricht der Reihenfolge der Datensätze. Jedes Unterfeld enthält 2 Informationselemente. Das erste Informationselement dient zur Identifizierung des Datensatztyps. Das zweite ist der IDC des Datensatzes. Das Trennzeichen „US" wird verwendet, um die beiden Informationselemente voneinander abzugrenzen.

3.1.4. Feld 1.004: Type of Transaction (TOT)

Dieses Feld enthält ein Mnemonik aus 3 Buchstaben, das den Transaktionstyp bezeichnet. Diese Codes können sich von den Codes unterscheiden, die von anderen Anwendungen des ANSI/NIST-Standards verwendet werden.

CPS: Criminal Print-to-Print Search. Diese Transaktion ist eine Anfrage zu einer Suche, mit einem Datensatz, der in Verbindung mit einer Straftat steht, in einer Fingerabdruck-Datenbank. Die Fingerabdrücke der Person müssen als WSQ-komprimierte Bilder in der Datei enthalten sein.

Wird kein Treffer festgestellt (No-HIT), so sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz.

Bei einem Treffer (HIT) sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz,

— 1-14 Typ-4-Datensätze.

Der CPS-TOT wird in Tabelle A.6.1 (Anlage 6) zusammengefasst.

PMS: Print-to-Latent Search. Diese Transaktion wird verwendet, wenn ein Satz Fingerabdrücke mit einer Datenbank abgeglichen werden soll, die nichtidentifizierte Fingerabdruckspuren enthält. Die Antwort enthält die Hit/No-Hit-Entscheidung des abgefragten AFIS-Systems. Wenn multiple nichtidentifizierte Fingerabdruckspuren vorliegen, sind multiple SRE-Transaktionen das Ergebnis, mit einer Fingerabdruckspur pro Transaktion. Die Fingerabdrücke der Person müssen als WSQ-komprimierte Bilder in der Datei enthalten sein.

Wird kein Treffer festgestellt (No-HIT), so sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz.

Bei einem Treffer (HIT) sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz,

— 1 Typ-13-Datensatz.

Der PMS-TOT wird in Tabelle A.6.1 (Anlage 6) zusammengefasst.

MPS: Latent-to-Print Search. Diese Transaktion wird verwendet, wenn eine Fingerabdruckspur gegen eine Fingerabdruck-Datenbank abgeglichen werden soll. In der Datei müssen die Informationen zu den Minutien der Fingerabdruckspur und das Bild (WSQ-komprimiert) enthalten sein.

Wird kein Treffer festgestellt (No-HIT), so sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz.

Bei einem Treffer (HIT) sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz,

— 1 Typ-4- oder Typ-15-Datensatz.

Der MPS-TOT wird in Tabelle A.6.4 (Anlage 6) zusammengefasst.

MMS: Latent-to-Latent Search. Bei dieser Transaktion enthält die Datei eine Fingerabdruckspur, die gegen eine Datenbank mit nichtidentifizierten Fingerabdruckspuren abgeglichen werden soll, um Bezüge zwischen verschiedenen Tatorten festzustellen. In der Datei müssen die Informationen zu den Minutien der Fingerabdruckspur und das Bild (WSQ-komprimiert) enthalten sein.

Wird kein Treffer festgestellt (No-HIT), so sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz.

Bei einem Treffer (HIT) sind die folgenden logischen Datensätze das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz,

— 1 Typ-13-Datensatz.

Der MMS-TOT wird in Tabelle A.6.4 (Anlage 6) zusammengefasst.

SRE: Diese Transaktion wird von der Empfangsstelle als Antwort auf die Suchanfrage mit daktyloskopischem Material rückübermittelt. Die Antwort enthält die Hit/No-Hit-Entscheidung des angefragten AFIS-Systems. Bei multiplen Kandidaten sind multiple SRE-Transaktionen das Ergebnis, mit einem Kandidaten pro Transaktion.

Der SRE-TOT wird in Tabelle A.6.2 (Anlage 6) zusammengefasst.

ERR: Diese Transaktion wird von der AFIS-Empfangsstelle rückübermittelt, um einen Transaktionsfehler anzuzeigen. Sie enthält ein Nachrichtenfeld (ERM), mit dem der festgestellte Fehler angegeben wird. Die folgenden logischen Datensätze sind das Ergebnis:

— 1 Typ-1-Datensatz,

— 1 Typ-2-Datensatz.

Der ERR-TOT wird in Tabelle A.6.3 (Anlage 6) zusammengefasst.

Tabelle 2: Zulässige Codes bei Transaktionen

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

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

Schlüssel:

M = Obligatorisch (Mandatory).
M* = Nur einer der beiden Datensatztypen kann aufgenommen werden.
O = Fakultativ (Optional).
C = Abhängig davon, ob Daten vorliegen.
— = Nicht zulässig.
1* = Abhängig von Legacy-Systemen.

3.1.5. Feld 1.005: Date of Transaction (DAT)

Dieses Feld gibt das Datum an, an dem die Transaktion gesendet wurde, und muss der ISO-Standard Schreibweise YYYYMMDD entsprechen,

wobei YYYY das Jahr, MM den Monat und DD den Tag bezeichnet. Vorangestellte Nullen werden bei 1-stelligen Zahlen verwendet. So steht beispielsweise „19931004" für den 4. Oktober 1993.

3.1.6. Feld 1.006: Priority (PRY)

Dieses fakultative Feld legt mit Stufen von 1 bis 9 die Priorität der Anfrage fest. „1" ist die höchste Prioritätsstufe und „9" die niedrigste Prioritätsstufe. Transaktionen der Prioritätsstufe „1" sind unverzüglich zu bearbeiten.

3.1.7. Feld 1.007: Destination Agency Identifier (DAI)

In diesem Feld wird der Empfänger für die Transaktion angegeben.

Es besteht aus 2 Informationselementen in folgendem Format: CC/*agency*.

Das erste Informationselement enthält den Ländercode nach dem Standard ISO-3166 und ist 2 alphanumerische Zeichen lang. Das zweite Element, *agency*, ist eine Freitextangabe der Empfangsstelle, die bis zu 32 alphanumerische Zeichen lang sein kann.

3.1.8. Feld 1.008: Originating Agency Identifier (ORI)

In diesem Feld wird der Absender der Datei angegeben; es hat das gleiche Format wie das DAI-Feld (Feld 1.007).

3.1.9. Feld 1.009: Transaction Control Number (TCN)

Dies ist eine Kontrollnummer zu Referenzzwecken. Sie sollte vom Computer generiert werden und folgendes Format haben: YYSSSSSSSSA.

Dabei steht YY für das Jahr der Transaktion, SSSSSSSS ist eine 8-stellige Seriennummer, und A ist ein Prüfzeichen, das nach dem Verfahren in Anlage 2 generiert wird.

Ist keine TCN vorhanden, so wird das Feld YYSSSSSSSS mit Nullen ausgefüllt und das Prüfzeichen wie oben angegeben generiert.

3.1.10. Feld 1.010: Transaction Control Response (TCR)

In der Antwort auf eine übermittelte Anfrage wird dieses fakultative Feld die Transaction Control Number (TCN) der Anfragenachricht enthalten. Es hat daher das gleiche Format wie ein TCN-Feld (Feld 1.009).

3.1.11. Feld 1.011: Native Scanning Resolution (NSR)

In diesem Feld wird die native Scan-Auflösung des Aufnahmesystems angegeben. Die Auflösung wird in Form von 2 Ziffern, gefolgt von einem Dezimalpunkt und 2 weiteren Ziffern angegeben.

Bei allen Transaktionen nach dem Beschluss 2008/615/JI beträgt die Abtastrate 500 Pixel/Inch oder 19,68 Pixel/mm.

3.1.12. Feld 1.012: Nominal Transmitting Resolution (NTR)

In diesem Feld mit 5 Bytes wird die nominale Übertragungsauflösung der übermittelten Bilder angegeben. Die Auflösung wird in Pixel/mm im gleichen Format wie das NSR-Feld angegeben (Feld 1.011).

3.1.13. Feld 1.013: Domain Name — DOM

In diesem obligatorischen Feld wird der Domänenname für die benutzerdefinierte Implementierung des Typ-2-Datensatzes angegeben. Es besteht aus 2 Informationselementen und lautet: „INT-I{US}4.22{GS}".

3.1.14. Feld 1.014: Greenwich Mean Time (GMT)

Dieses obligatorische Feld bietet einen Mechanismus, mit dem das Datum und die Uhrzeit in universellen Einheiten der Greenwich Mean Time (GMT) ausgedrückt werden kann. Sofern es verwendet wird, enthält das GMT-Feld das universelle Datum zusätzlich zu dem lokalen Datum in Feld 1.005 (DAT). Mit der Verwendung des GMT-Feldes fallen Unvereinbarkeiten der Ortszeit weg, die bestehen, wenn eine Transaktion und ihre Antwort zwischen zwei Orten übertragen werden, zwischen denen mehrere Zeitzonen liegen. GMT bietet unabhängig von den Zeitzonen ein universelles Datum und eine Uhrzeit im 24-Stunden-Modus. Die Darstellung ist „CCYYMMDDHHMMSSZ", eine Kette mit 15 Zeichen, bei der es sich um die Verkettung des Datums mit der GMT, abgeschlossen durch ein „Z", handelt. Die Zeichen „CCYY" stehen für das Jahr der Transaktion, die Zeichen „MM" für die Zehner- und Einerstellen des Monats, die Zeichen „DD" für die Zehner- und Einerstellen des Monatstags, die Zeichen „HH" für die Stunde, die Zeichen „MM" für die Minute und die Zeichen „SS" für die Sekunde. Das vollständige Datum darf nicht über das aktuelle Datum hinausgehen.

4. ***Typ-2-Datensatz: Beschreibender Text***

Die Struktur des größten Teils dieses Datensatzes entspricht nicht dem ursprünglichen ANSI/NIST-Standard. Der Datensatz enthält Informationen von besonderem Interesse für die Stellen, die die Datei aussenden oder empfangen. Um zu gewährleisten, dass die miteinander kommunizierenden daktyloskopischen Systeme kompatibel sind, dürfen nur die unten angegebenen Felder in dem Datensatz enthalten sein. Dieses Dokument gibt an, welche Felder obligatorisch und welche fakultativ sind, und es legt ferner die Struktur der einzelnen Felder fest.

4.1. *Felder für Typ-2-Datensätze*

4.1.1. Feld 2.001: Logical Record Length (LEN)

Dieses obligatorische Feld enthält die Länge dieses Typ-2-Datensatzes und gibt die Gesamtmenge von Bytes an; darin enthalten sind alle Zeichen in allen Feldern des Datensatzes sowie die Informationstrennzeichen.

4.1.2. Feld 2.002: Image Designation Character (IDC)

Das in diesem obligatorischen Feld enthaltene IDC ist eine ASCII-Darstellung des IDC, das im Feld Dateiinhalt (File Content — CNT) des Typ-1-Datensatzes (Feld 1.003) definiert ist.

4.1.3. Feld 2.003: System Information (SYS)

Dieses Feld ist obligatorisch und enthält 4 Bytes, die angeben, welcher Version der Interpol-Implementierung (INT-I) dieser Typ-2-Datensatz entspricht.

Die ersten 2 Bytes geben die führende Nummer der Version an, während die weiteren 2 Bytes die Revisionsnummer angeben. Diese Implementierung basiert beispielsweise auf der INT-I-Version 4 Revision 22 und würde somit als „0422" dargestellt werden.

4.1.4. Feld 2.007: Case Number (CNO)

Diese Nummer wird von der örtlichen Daktyloskopiestelle einer Sammlung von Fingerabdruckspuren, die an einem Tatort gesichert wurden, zugeordnet. Dabei wird folgendes Format verwendet: CC/*number*

wobei CC der Interpol-Ländercode ist (2 alphanumerische Zeichen) und „number" den jeweiligen Leitlinien vor Ort entspricht und aus bis zu 32 alphanumerischen Zeichen bestehen kann.

Mit diesem Feld kann das System Fingerabdruckspuren identifizieren, die mit einer bestimmten Straftat verbunden sind.

4.1.5. Feld 2.008: Sequence Number (SQN)

Dieses Feld gibt jede Sequenz von Fingerabdruckspuren im Rahmen eines bestimmten Falls an. Es kann aus bis zu 4 numerischen Zeichen bestehen. Eine Sequenz ist eine Fingerabdruckspur oder eine Reihe von Fingerabdruckspuren, die zum Zwecke der Archivierung und/oder Suche zusammengefasst werden. Aufgrund dieser Definition müssen auch einzelne Fingerabdruckspuren eine Sequenznummer erhalten.

Dieses Feld kann zusammen mit dem Feld MID (Feld 2.009) benutzt werden, um eine bestimmte Fingerabdruckspur innerhalb einer Sequenz zu identifizieren.

4.1.6. Feld 2.009: Latent Identifier (MID)

Dieses Feld bezeichnet eine einzelne Fingerabdruckspur innerhalb einer Sequenz. Der Wert besteht aus einem einzelnen oder 2 Buchstaben, wobei „A" die erste Fingerabdruckspur und „B" die zweite Fingerabdruckspur bezeichnet, bis zu maximal „ZZ". Dieses Feld wird analog zur Fingerabdruckspur-Sequenznummer verwendet (siehe Beschreibung von Feld 2.008 SQN).

4.1.7. Feld 2.010: Criminal Reference Number (CRN)

Dies ist eine eindeutige Referenznummer, die eine nationale Behörde einer Person zuteilt, die zum ersten Mal beschuldigt wird, eine Straftat begangen zu haben. Innerhalb eines Landes hat eine Person nie mehr als eine CRN, und es haben nie zwei Personen dieselbe CRN. Eine Person kann jedoch Straftäter-Referenznummern in mehreren Ländern haben; in diesem Fall unterscheiden sie sich durch den Ländercode.

Für das CRN-Feld wird folgendes Format verwendet: CC/*number*

wobei CC der Ländercode nach ISO 3166 ist (2 alphanumerische Zeichen) und „number" den jeweiligen nationalen Leitlinien der ausstellenden Behörde entspricht und aus bis zu 32 alphanumerischen Zeichen bestehen kann.

Für Transaktionen gemäß dem Beschluss 2008/615/JI wird dieses Feld für die nationale Straftäter-Referenznummer der Behörde, die den Datensatz erstellt, verwendet; diese Nummer ist mit den Abbildungen in den Typ-4- oder Typ-15-Datensätzen verknüpft.

4.1.8. Feld 2.012: Miscellaneous Identification Number (MN1)

Dieses Feld enthält die im Rahmen einer CPS- oder PMS-Transaktion übermittelte CRN (Feld 2.010) ohne den vorangestellten Ländercode.

4.1.9. Feld 2.013: Miscellaneous Identification Number (MN2)

Dieses Feld enthält die im Rahmen einer MPS- oder MMS-Transaktion übermittelte CNO (Feld 2.007) ohne den vorangestellten Ländercode.

4.1.10. Feld 2.014: Miscellaneous Identification Number (MN3)

Dieses Feld enthält die im Rahmen einer MPS- oder MMS-Transaktion übermittelte SQN (Feld 2.008).

4.1.11. Feld 2.015: Miscellaneous Identification Number (MN4)

Dieses Feld enthält das im Rahmen einer MPS- oder MMS-Transaktion übermittelte MID (Feld 2.009).

4.1.12. Feld 2.063: Additional Information (INF)

Bei einer SRE-Transaktion im Anschluss an eine PMS-Anfrage enthält dieses Feld Informationen über den Finger, der den möglichen Treffer (HIT) ergeben hat. Das Feld hat folgendes Format:

NN wobei *NN* der in Tabelle 5 definierte Fingerpositionscode ist (2 Zeichen).

In allen anderen Fällen ist das Feld fakultativ. Es besteht aus bis zu 32 alphanumerischen Zeichen und kann zusätzliche Informationen über die Suchanfrage enthalten.

4.1.13. Feld 2.064: Respondents List (RLS)

Dieses Feld enthält mindestens 2 Unterfelder. Das erste Unterfeld beschreibt die Art der durchgeführten Suche anhand der aus 3 Buchstaben bestehenden Mnemonik, die die Art der Transaktion im TOT (Feld 1.004) bezeichnen. Das zweite Unterfeld enthält ein einziges Zeichen. Ein „I" bedeutet, dass ein HIT gefunden wurde, und ein „N" gibt an, dass keine Übereinstimmung gefunden wurde (NOHIT). Das dritte Unterfeld enthält die Sequenz-Kennnummer für die gefundenen Kandidaten und die Gesamtzahl der Kandidaten, getrennt durch einen Schrägstrich. Bei mehreren Kandidaten werden entsprechend mehrere Mitteilungen gesendet.

Bei einem möglichen HIT enthält das vierte Unterfeld die Trefferzahl (score) aus bis zu 6 Zeichen. Wurde der HIT überprüft, so enthält dieses Teilfeld den Wert „999999".

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

Teilt das AFIS der ersuchten Stelle keine Trefferzahlen (score) mit, so sollte an der entsprechenden Stelle die Trefferzahl Null verwendet werden.

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

Dieses Feld enthält aus den Transaktionen hervorgehende Fehlermeldungen, die im Rahmen einer Fehlertransaktion an die ersuchende Stelle zurückgesandt werden.

Tabelle 3: Fehlermeldungen

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

Fehlermeldungen im Bereich zwischen 100 und 199:

Diese Fehlermeldungen beziehen sich auf die Validierung der ANSI/NIST-Datensätze und sind wie folgt definiert:

<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>…

wobei

— error_code ein Code ist, der sich ausschließlich auf einen spezifischen Grund bezieht (siehe Tabelle 3);

— field_id die ANSI/NIST-Feldnummer des nicht korrekten Feldes ist (z. B. 1.001, 2.001 usw.), und zwar im Format <record_type>.field_id>.sub_field_id>;

— dynamic text eine genauere Beschreibung des Fehlers ist;

— LF ein Zeilenvorschub (Line Feed) als Trennung zwischen Fehlern ist, wenn mehrere Fehler auftreten;

— für Typ-1-Datensätze das IDC als „-1“ definiert wird.

Beispiel:

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

Dieses Feld ist bei Fehlertransaktionen obligatorisch.

4.1.15. Feld 2.320: Expected Number of Candidates (ENC)

Dieses Feld enthält die von der anfragenden Stelle erwartete Höchstzahl von Kandidaten zur Überprüfung. Der Wert des ENC-Feldes darf die in Tabelle 11 definierten Werte nicht übersteigen.

5. *Typ-4-Datensatz: Hochauflösendes Bild in Grautönen*

Typ-4-Datensätze sind binär codiert, sie haben keine ASCII-Zeichen. Daher wird jedem Feld eine Position im Datensatz zugewiesen, was bedeutet, dass alle Felder obligatorisch zu besetzen sind.

Der Standard ermöglicht es, sowohl Bildgröße als auch Auflösung im Datensatz zu spezifizieren. Typ-4-Datensätze werden zur Einbindung daktyloskopischer Bilddaten benötigt, die mit einer nominalen Pixeldichte von 500 bis 520 Pixel/Inch übertragen werden. Bevorzugte Pixelrate bei neuen Grafiken ist 500 Pixel/Inch oder 19,68 Pixel/mm. Eine Dichte von 500 Pixel/Inch wird von der INT-I-Norm vorgeschrieben; allerdings können vergleichbare Systeme auch ohne Einhaltung dieser bevorzugten Pixelrate miteinander kommunizieren, sofern sich die Rate zwischen 500 und 520 Pixel/Inch bewegt.

5.1. *Felder von Typ-4-Datensätzen*

5.1.1. Feld 4.001: Logical record length (LEN)

Dieses 4-Byte-Feld enthält die Länge des Typ-4-Datensatzes und gibt die Gesamtanzahl von Bytes, d. h. jedes Byte von jedem im Datensatz enthaltenen Feld, an.

5.1.2. Feld 4.002: Image designation character (IDC)

Hierbei handelt es sich um die 1-Byte-Binärdarstellung der IDC-Nummer die im Typ 1 festgelegt wurde.

5.1.3. Feld 4.003: Impression type (IMP)

Der Abdrucktyp ist ein 1-Byte-Feld, das das sechste Byte des Datensatzes belegt.

Tabelle 4: Fingerabdrucktyp

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

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

5.1.4. Feld 4.004: Finger position (FGP)

Dieses Feld mit einer festen Länge von 6 Bytes belegt die siebte bis zwölfte Byte-Position im Typ-4-Datensatz. Es enthält die möglichen Fingerabdruckpositionen und beginnt mit dem äußersten linken Byte (Byte 7 des Datensatzes). Die bekannte bzw. wahrscheinlichste Fingerabdruckposition wird der Tabelle 5 entnommen. Maximal 5 weitere Finger können durch Aufnahme der alternativen Fingerabdruckpositionen in den verbleibenden 5 Bytes unter Verwendung desselben Formats referenziert werden. Sollen weniger als 5 Referenzwerte für Fingerabdruckpositionen verwendet werden, werden die ungenutzten Bytes mit dem Binärwert 255 belegt. Um alle Fingerabdruckpositionen zu referenzieren, wird der Code 0 (= unbekannt) verwendet.

Tabelle 5: Fingerabdruckpositionscode und maximale Größe

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

Für Tatortspuren sollten nur die Codes 0 bis 10 verwendet werden.

5.1.5. Feld 4.005: Image scanning resolution (ISR)

Dieses 1 Byte große Feld belegt das 13. Byte eines Typ-4-Datensatzes. Enthält es „0“, so wurde das Bild mit der bevorzugten Scan-Rate von 19,68 Pixel/mm (500 Pixel/Inch) abgetastet. Enthält es „1“, dann wurde das Bild mit einer anderen Scan-Rate als der für den Typ-1-Datensatz empfohlenen Scan-Rate abgetastet.

5.1.6. Feld 4.006: Horizontal line length (HLL)

Dieses Feld belegt die Bytes 14 und 15 im Typ-4-Datensatz. Es legt die Anzahl der Pixel in jeder horizontal verlaufenden Linie (scan line) fest. Die höchstwertige Stelle ist das erste Byte.

5.1.7. Feld 4.007: Vertical line length (VLL)

Dieses Feld erfasst in den Bytes 16 und 17 die im Bild vorhandene Anzahl vertikaler Linien (scan lines). Die höchstwertige Stelle ist das erste Byte.

5.1.8. Feld 4.008: Gray-scale Compression Algorithm (GCA)

Dieses Feld erfasst den zur Bilddatencodierung verwendeten Graustufenkomprimierungsalgorithmus. Hierbei gibt Binär „1" an, dass die WSQ-Komprimierung (Anlage 7) verwendet wurde.

5.1.9. Feld 4.009: Image

Dieses Feld enthält einen Bytestrom, der das Bild darstellt. Natürlich richtet sich seine Struktur nach dem verwendeten Komprimierungsalgorithmus.

6. ***Typ-9-Datensatz: Minutiendatensatz***

Typ-9-Datensätze enthalten ASCII-Text mit einer Beschreibung der Minutien und zugehörigen codierten Informationen zu einer Spur. Im Hinblick auf die Spurensuche gibt es keine Beschränkung für Typ-9-Datensätze in einer Datei, da jeder Datensatz zu einer anderen Ansicht oder Spur gehört.

6.1. *Minutienextraktion*

6.1.1. Identifizierung des Minutientyps

Dieser Standard legt drei Bezeichner fest, die zur Beschreibung des Minutientyps verwendet werden. Sie sind in Tabelle 6 aufgeführt. Ein Papillarlinienende wird als Typ 1, eine Gabelung als Typ 2 bezeichnet. Lässt sich eine Minutie nicht eindeutig einem der beiden vorgenannten Typen zuordnen, wird sie als Typ 0 „Sonstige" bezeichnet.

Tabelle 6: Minutientypen

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Minutienposition und -typ

Damit Schablonen die Anforderungen des Abschnitts 5 der Norm ANSI INCITS 378-2004 erfüllen, ist für die Bestimmung der Position (Lage und Neigung) jeder einzelnen Minutie die folgende Methode zu verwenden, die eine Verbesserung gegenüber der zurzeit geltenden Norm INCITS 378-2004 darstellt.

Bei einer Minutie, die ein Papillarlinienende darstellt, bildet der Verzweigungspunkt im Talbereich des Papillarlinienbildes unmittelbar in Höhe des Papillarlinienendes den Minutienort. Sind die drei Stränge im Talbereich zu einer 1 Pixel dünnen Papillarlinie verdünnt, dann bildet der Kreuzungspunkt den Minutienort. Analog dazu ist die Minutienposition einer Gabelung die Erhöhung im Gabelungspunkt. Wenn sich jeder der drei Linienstränge zu einer 1 Pixel dünnen Papillarline verjüngt, dann bildet der Punkt, an dem die drei Stränge sich kreuzen, den Minutienort.

Nachdem alle Papillarlinienenden in Gabelungen umgewandelt sind, werden alle Minutien des daktyloskopischen Bildes als Gabelungen dargestellt. Die Pixelkoordinaten x und y des Schnittpunkts der drei Stränge jeder Minutie können direkt formatiert werden. Die Bestimmung der Minutienrichtung kann aus jedem Papillarlinienbild abgeleitet werden. Die drei Stränge jeder Papillarliniengabelung müssen untersucht und der Endpunkt jedes Strangs muss ermittelt werden. Abbildung 6.1.2 zeigt die Methoden zur Bestimmung des Strangendes mit einer Scan-Auflösung von 500 ppi.

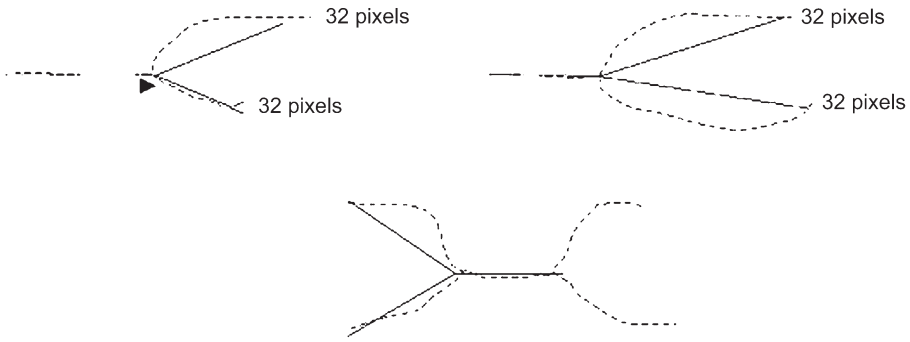
Die Endung wird nach dem zuerst eintretenden Ereignis ermittelt. Die Pixelzählung basiert auf einer Scan-Auflösung von 500 ppi. Unterschiedliche Scan-Auflösungen würden auch unterschiedliche Pixelzählungen bedeuten:

— eine Distanz von 0,064″ (der 32. Pixel);

— das Ende des Skelettlinienstrangs, das sich in einer Distanz zwischen 0,02″ und 0,064″ (vom 10. bis 32. Pixel) befindet; kürzere Stränge werden nicht verwendet;

— eine zweite Gabelung befindet sich auf einer Strecke von 0,064″ (vor dem 32. Pixel).

Abbildung 6.1.2



Der Minutienwinkel wird bestimmt, indem drei virtuelle Strahlen, ausgehend von der Gabelung bis zum Ende jedes Strangs, konstruiert werden. Der kleinste der drei von den Strahlen gebildeten Winkel wird halbiert und ergibt so die Minutienrichtung.

6.1.3. Koordinatensystem

Das zur Darstellung der Minutien eines Fingerabdrucks verwendete Koordinatensystem ist ein kartesisches System. Die Minutienorte werden durch ihre x- und y-Koordinaten dargestellt. Koordinatenursprung ist die linke obere Ecke des Originalbildes, wobei x nach rechts, y nach unten ansteigende Werte aufweist. Sowohl die x- als auch die y-Koordinate einer Minutie ist vom Ursprung ausgehend in Pixeleinheiten darzustellen. Es sei darauf verwiesen, dass Ursprungsort und Maßeinheiten nicht der Konvention für Begriffsbestimmungen der Typ-9-Datensätze aus der Norm ANSI/NIST-ITL 1-2000 entsprechen.

6.1.4. Minutienrichtung

Winkel werden im üblichen mathematischen Format ausgedrückt, d. h. Nullwinkel rechts, ansteigende Winkel entgegen Uhrzeigerrichtung. Erfasst wird bei Papillarlinienenden die Richtung entlang der Papillarlinie und bei Gabelungen die Richtung zur Mitte des Talbereichs. Diese Konvention ist um 180 Grad versetzt gegenüber der Winkelkonvention, wie sie in den Begriffsbestimmungen für Typ-9-Datensätze in der Norm ANSI/NIST-ITL 1-2000 beschrieben ist.

6.2. *Felder von Typ-9-Datensätzen im INCITS-378-Format*

Alle Felder von Typ-9-Datensätzen sind als ASCII-Text zu speichern. Binärfelder sind in diesem nummerierten Datensatz nicht zulässig.

6.2.1. Feld 9.001: Logical record length (LEN)

Dieses obligatorische ASCII-Feld enthält die Länge des Datensatzes und gibt die Gesamtanzahl von Bytes, d. h. auch jedes Zeichen von jedem im Datensatz enthaltenen Feld, an.

6.2.2. Feld 9.002: Image designation character (IDC)

Dieses obligatorische 2-Byte-Feld ist für die Kennzeichnung und Lokalisierung der Minutiendaten zu verwenden. Der in diesem Feld enthaltene IDC muss mit dem IDC übereinstimmen, der sich in dem Feld „Dateiinhalt" des Typ-1-Datensatzes befindet.

6.2.3. Feld 9.003: Impression type (IMP)

Dieses obligatorische 1-Byte-Feld beschreibt, auf welche Weise die daktyloskopischen Bildinformationen gewonnen wurden. Der ASCII-Wert des aus der Tabelle 4 ausgewählten Codes wird zur Kennzeichnung des Abdrucktyps in dieses Feld eingegeben.

6.2.4. Feld 9.004: Minutiæ format (FMT)

Dieses Feld enthält ein „U" als Hinweis darauf, dass die Minutien nach dem M1-378-Standard formatiert wurden. Zwar können die Daten nach dem M1-378-Standard codiert werden, doch müssen alle Datenfelder des Typ-9-Datensatzes weiterhin als ASCII-Textfelder formatiert sein.

6.2.5. Feld 9.126: CBEFF information

Dieses Feld enthält 3 Informationselemente. Das erste Informationselement enthält den Wert „27" (0x1B). Hierbei handelt es sich um die Kennung des CBEFF-Formatinhabers, die von der International Biometric Industry Association (IBIA) dem Technischen Ausschuss M1 von INCITS zugewiesen wurde. Das Zeichen <US> soll dieses Informationselement von dem CBEFF-Formattyp abgrenzen, dem ein Wert „513" (0x0201) zugewiesen wurde,

um anzugeben, dass dieser Datensatz nur Daten über Ort und Neigung ohne sonstige Daten des erweiterten Datenblocks enthält. Das Zeichen <US> grenzt dieses Datenelement von der CBEFF-Produktkennung (PID) ab, die auf den „Eigentümer" der Codiereinrichtung hinweist. Dieser Wert wird vom Lieferant festgelegt. Er kann von der IBIA-Website (www.ibia.org) abgerufen werden, sofern er veröffentlicht wird.

6.2.6. Feld 9.127: Capture equipment identification

Dieses Feld enthält 2 durch das Zeichen <US> getrennte Informationselemente. Das erste Informationselement erhält die Zeichen „APPF", wenn zertifiziert wurde, dass das für die Bilderfassung zuerst eingesetzte Gerät die Anforderungen des Anhangs F (IAFIS Image Quality Specification, January 29, 1999) der Norm CJIS-RS-0010 (FBI-Spezifikation zur elektronischen Übertragung von Fingerabdrücken) erfüllt. Andernfalls hat das Informationselement den Wert „NONE". Das zweite Informationselement enthält die Erfassungsgerätekennung, bei der es sich um die dem Lieferer zugewiesene Erzeugnisnummer des Erfassungsgerätes handelt. Der Wert „0" gibt an, dass keine Erfassungsgerätekennung gemeldet wurde.

6.2.7. Feld 9.128: Horizontal line length (HLL)

Dieses obligatorische ASCII-Feld enthält die Anzahl der Pixel einer einzelnen horizontalen Zeilenlänge des übertragenen Bildes. Das maximale Horizontalmaß ist auf 65 534 Pixel begrenzt.

6.2.8. Feld 9.129: Vertical line length (VLL)

Dieses obligatorische ASCII-Feld enthält die Anzahl der im übertragenen Bild enthaltenen horizontalen Zeilen. Das maximale Vertikalmaß ist auf 65 534 Pixel begrenzt.

6.2.9. Feld 9.130: Scale units (SLC)

Dieses obligatorische ASCII-Feld gibt die Maßeinheiten für die Angabe der Bildabtastfrequenz (Pixeldichte) an. Eine „1" in diesem Feld bedeutet Pixel/Inch, eine „2" steht für Pixel/cm. Eine „0" in diesem Feld bedeutet, dass keine Maßeinheit vorgegeben wurde. In diesem Fall liefert der Quotient aus HPS/VPS das Seitenverhältnis.

6.2.10. Feld 9.131: Horizontal pixel scale (HPS)

Dieses obligatorische ASCII-Feld gibt die ganzzahlige Pixeldichte in horizontaler Richtung an, wenn im SLC-Feld eine „1" oder eine „2" steht. Andernfalls gibt es die horizontale Komponente des Seitenverhältnisses an.

6.2.11. Feld 9.132: Vertical pixel scale (VPS)

Dieses obligatorische ASCII-Feld gibt die ganzzahlige Pixeldichte in vertikaler Richtung an, wenn im SLC-Feld eine „1" oder eine „2" steht. Andernfalls gibt es die vertikale Komponente des Seitenverhältnisses an.

6.2.12. Feld 9.133: Finger view

Dieses obligatorische Feld enthält die zu diesem Datensatz gehörende Fingernummer. Die Nummer beginnt bei „0" und geht in Einerschritten bis „15".

6.2.13. Feld 9.134: Finger position (FGP)

Dieses Feld enthält den Code der Fingerabdruckposition, die die Daten zu diesem Typ-9-Datensatz erzeugt hat. Ein Code zwischen 1 und 10 aus Tabelle 5 bzw. der entsprechende Handabdruckcode aus Tabelle 10 ist für die Angabe der Finger- bzw. Handabdruckposition zu verwenden.

6.2.14. Feld 9.135: Finger quality

Dieses Feld gibt die Qualität der Daten der Fingerminutien an; die Werte hierfür liegen zwischen 0 und 100. Die Zahl erfasst die gesamte Qualität des Fingerdatensatzes und spiegelt die Qualität des Originalbilds, der Extraktion der Minutien und weitere Arbeitsabläufe, die den Minutiendatensatz beeinflussen können, wider.

6.2.15. Feld 9.136: Number of minutiæ

Dieses obligatorische Feld nennt die Zahl der in diesem Datensatz erfassten Minutien.

6.2.16. Feld 9.137: Finger minutiæ data

Dieses obligatorische Feld enthält 6 durch das Zeichen <US> getrennte Informationselemente. Es besteht aus mehreren Unterfeldern, die jeweils die Details zu den einzelnen Minutien enthalten. Die Gesamtzahl der Minutienunterfelder muss mit der in Feld 136 angegebenen Zahl übereinstimmen. Das erste Informationselement ist die Minutienindexzahl, die mit „1“ beginnt und sich für jede weitere Minutie des Fingerabdrucks um „1“ erhöht. Das zweite Informationselement stellt die Pixelkoordinate x, das dritte die Pixelkoordinate y der Minutien dar. Das vierte Informationselement ist der in 2-Grad-Schritten erfasste Minutienwinkel. Dieser Wert darf nicht negativ sein; er reicht von 0 bis 179. Das fünfte Informationselement ist der Minutientyp. Ein Wert „0“ bezeichnet den Minutientyp „SONSTIGE“, der Wert „1“ ein Papillarlinienende und der Wert „2“ eine Gabelung. Das sechste Informationselement bezeichnet die Qualität der jeweiligen Minutie. Die Zahl reicht vom Mindestwert 1 bis zum Höchstwert 100. Ein Wert „0“ besagt, dass keine Qualitätsangabe vorliegt. Jedes Unterfeld wird vom nächsten durch das Trennzeichen <RS> getrennt.

6.2.17. Feld 9.138: Ridge count information

Dieses Feld besteht aus einer Reihe von Unterfeldern, die jeweils 3 Informationselemente enthalten. Das erste Informationselement des ersten Unterfelds gibt die Methode zur Bestimmung der Papillarlinienanzahl an. Eine „0“ bedeutet, dass keine Vorgaben zur Methode zur Bestimmung der Papillarlinienanzahl oder zur Reihenfolge der Papillarlinienzahl bestehen. Eine „1“ bedeutet, dass für jede zentrale Minutie Linienzähldaten bis zur nächsten Nachbarminutie in den 4 Quadranten extrahiert und Linienzählungen für jede zentrale Minutie gemeinsam aufgelistet werden. Eine „2“ bedeutet, dass für jede zentrale Minutie Linienzähldaten bis zur nächsten Nachbarminutie in den 8 Oktanten extrahiert und Linienzählungen für jede zentrale Minutie gemeinsam aufgelistet werden. Die verbleibenden 2 Informationselemente des ersten Teilfelds enthalten jeweils „0“. Die Informationselemente werden durch das Trennzeichen <US> voneinander getrennt. Die folgenden Unterfelder enthalten als erstes Informationselement die Indexnummer der zentralen Minutie, als zweites Informationselement die Indexnummer der Nachbarminutie und als drittes Informationselement die Zahl der gekreuzten Papillarlinien. Die Unterfelder werden durch das Trennzeichen <RS> voneinander getrennt.

6.2.18. Feld 9.139: Core information

Dieses Feld besteht aus einem Unterfeld für jeden im Originalbild enthaltenen Kern. Jedes Unterfeld enthält 3 Informationselemente. Die ersten beiden Informationselemente geben die Pixelkoordinaten x bzw. y an. Das dritte Informationselement enthält den Winkel des Kerns, der in 2-Grad-Schritten erfasst wird. Der Wert darf nicht negativ sein; er reicht von 0 bis 179. Mehrere Kerne werden durch das Trennzeichen <RS> voneinander getrennt.

6.2.19. Feld 9.140: Delta information

Dieses Feld besteht aus einem Unterfeld für jedes im Originalbild enthaltene Delta. Jedes Unterfeld enthält 3 Informationselemente. Die ersten beiden Informationselemente geben die Pixelkoordinaten x bzw. y an. Das dritte Informationselement enthält den Winkel des Deltas, der in 2-Grad-Schritten erfasst wird. Der Wert darf nicht negativ sein; er reicht von 0 bis 179. Mehrere Kerne werden durch das Trennzeichen <RS> voneinander getrennt.

7. ***Typ-13-Datensatz mit Bildern von Fingerabdruck- und Handflächenabdruckspuren in variabler Auflösung***

Der Typ-13-Datensatz mit nummerierten Feldern enthält Bilddaten, die aus Bildern von Fingerabdruck- und Handflächenabdruckspuren erfasst wurden. Diese Bilder sollen an Stellen übermittelt werden, die die gewünschten Merkmalsinformationen aus diesen Bildern entweder automatisch oder durch Eingriff ihrer Mitarbeiter für eine Weiterverarbeitung extrahieren.

Angaben zur gewählten Scan-Auflösung, Bildgröße und zu sonstigen erforderlichen Parametern für die Bildverarbeitung werden im Datensatz in nummerierten Feldern erfasst.

Tabelle 7: Aufbau des Typ-13-Datensatzes

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

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

Zeichenlegende: N = numerisch; A = alphabetisch; AN = alphanumerisch; B = binär.

7.1. *Felder von Typ-13-Datensätzen*

In den nachfolgenden Absätzen werden die Daten beschrieben, die in jedem Feld eines Typ-13-Datensatzes enthalten sind.

In Typ-13-Datensätzen sind die Daten in nummerierten Feldern einzugeben. Es ist notwendig, dass die Reihenfolge für die ersten beiden Felder des Datensatzes eingehalten wird und dass das Feld mit den Bilddaten das letzte physikalische Feld im Datensatz bildet. Zu jedem Feld des Typ-13-Datensatzes enthält Tabelle 7 folgende Angaben: Bedingungscode (condition code) mit dem Wert „M“ (mandatory — obligatorisch) oder „O“ (optional — fakultativ), Feldnummer (field number), Zeichensatz (character type), Feldgröße (field size) und quantitative Begrenzung der Vorkommnisse (occurrance limits). Die letzte Spalte gibt anhand einer 3-stelligen Feldnummer die maximale Feldgröße in Bytes an. Wenn mehr Stellen für die Feldnummer verwendet werden, steigt auch die maximale Bytezahl. Die beiden Einträge unter „field size per occurrence“ umfassen alle im Feld verwendeten Trennzeichen. Unter „maximum byte count“ fallen die Feldnummer, die Information und alle Trennzeichen einschließlich des „GS“-Trennzeichens.

7.1.1. Feld 13.001: Logical record length (LEN)

Dieses obligatorische ASCII-Feld enthält die Gesamtzahl an Bytes im Typ-13-Datensatz. Das Feld 13.001 gibt die Datensatzlänge, einschließlich jedes Zeichens in jedem Feld des Datensatzes und der Trennzeichen, an.

7.1.2. Feld 13.002: Image designation character (IDC)

Dieses obligatorische ASCII-Feld wird verwendet, um die Spurbilddaten im Datensatz zu kennzeichnen. Dieser IDC muss mit dem IDC übereinstimmen, der im Feld Dateiinhalt (CNT) des Typ-1-Datensatzes angegeben ist.

7.1.3. Feld 13.003: Impression type (IMP)

Dieses aus 1 bzw. 2 Byte bestehende obligatorische ASCII-Feld gibt an, wie die Spurbildinformation gewonnen wurde. Der entsprechende Spurbildcode wird aus Tabelle 4 (Fingerabdruck) bzw. Tabelle 9 (Handabdruck) ausgewählt und in dieses Feld eingetragen.

7.1.4. Feld 13.004: Source agency (SRC)

Dieses obligatorische ASCII-Feld bezeichnet die Behörde oder Organisation, die das im Datensatz enthaltene Spurenbild ursprünglich erfasst hat. In der Regel enthält dieses Feld die Absenderkennung (Originating Agency Identifier — ORI) der Stelle, die das Bild erfasst hat. Das Feld besteht aus 2 Datenelementen, die das Format CC/*agency* haben.

Das erste Datenelement enthält den Interpol-Ländercode, der sich aus 2 alphanumerischen Zeichen zusammensetzt. Das zweite Datenelement, *„agency"*, dient der freitextlichen Bezeichnung der betreffenden Stellen mit maximal 32 alphanumerischen Zeichen.

7.1.5. Feld 13.005: Latent capture date (LCD)

Dieses obligatorische ASCII-Feld gibt das Datum an, an welchem das im Datensatz enthaltene Spurenbild erfasst wurde. Das Datum besteht aus 8 Zeichen im Format CCYYMMDD. Die Zeichen CCYY geben das Jahr der Bilderfassung, die Zeichen MM die Zehner- und Einer-Stelle des Monats und die Zeichen DD die Zehner- und Einer-Stelle des Tags des entsprechenden Monats an. 20000229 bedeutet beispielsweise 29. Februar 2000. Das vollständige Datum muss ein gesetzliches Datum ergeben.

7.1.6. Feld 13.006: Horizontal line length (HLL)

Dieses obligatorische ASCII-Feld gibt die Pixelzahl einer einzelnen horizontalen Zeilenlänge des übertragenen Bildes an.

7.1.7. Feld 13.007: Vertical line length (VLL)

Dieses obligatorische ASCII-Feld gibt die Zahl der im übertragenen Bild enthaltenen horizontalen Zeilen an.

7.1.8. Feld 13.008: Scale units (SLC)

Dieses obligatorische ASCII-Feld nennt die Maßeinheiten für die Angabe der Bildabtastfrequenz (Pixeldichte). Eine „1" in diesem Feld bedeutet Pixel/Inch, eine „2" steht für Pixel/cm. Eine „0" in diesem Feld bedeutet, dass keine Maßeinheit vorgegeben wurde. In diesem Fall liefert der Quotient aus HPS/VPS das Seitenverhältnis.

7.1.9. Feld 13.009: Horizontal pixel scale (HPS)

Dieses obligatorische ASCII-Feld gibt die ganzzahlige Pixeldichte in horizontaler Richtung an, wenn im SLC-Feld eine „1" oder eine „2" steht. Andernfalls gibt es die horizontale Komponente des Seitenverhältnisses an.

7.1.10. Feld 13.010: Vertical pixel scale (VPS)

Dieses obligatorische ASCII-Feld gibt die ganzzahlige Pixeldichte in vertikaler Richtung an, wenn im SLC-Feld eine „1" oder eine „2" steht. Andernfalls gibt es die vertikale Komponente des Seitenverhältnisses an.

7.1.11. Feld 13.011: Compression algorithm (CGA)

Dieses obligatorische ASCII-Feld gibt den zur Komprimierung von Graustufenbildern verwendeten Algorithmus an. Siehe Komprimierungscodes in Anlage 7.

7.1.12. Feld 13.012: Bits per pixel (BPX)

Dieses obligatorische ASCII-Feld gibt die zur Darstellung eines Pixels verwendete Anzahl von Bits an. Für normale Graustufenwerte zwischen „0" und „255" wird in dieses Feld der Wert „8" eingetragen. Jeder größere Wert als „8" in diesem Feld bezeichnet einen Graustufenpixel mit höherer Präzision.

7.1.13. Feld 13.013: Finger/palm position (FGP)

Dieses obligatorische nummerierte Feld gibt eine oder mehrere mögliche Finger- oder Handflächenposition an, die der latenten Spur entsprechen können. Der Dezimalcodewert, der der bekannten oder wahrscheinlichsten Fingerposition bzw. Handflächenposition entspricht, ist der Tabelle 5 bzw. der Tabelle 10 zu entnehmen und als 1- oder 2-stelliges ASCII-Unterfeld einzugeben. Verweise auf zusätzliche Finger- und/oder Handflächenpositionen können durch Eingabe der alternierenden Positionscodes als mit dem „RS"-Trennzeichen abgetrennte Unterfelder aufgenommen werden. Der Code „0" für „Unknown Finger" (unbekannter Finger) wird zur Angabe jeder Fingerposition von 1 bis 10 angegeben. Der Code „20" für „Unknown Palm" (unbekannte Handfläche) wird zur Bezugnahme auf jede gelistete Fingerabdruckposition verwendet.

7.1.14. Felder 13.014-13.019: Reserved for future definition (RSV)

Diese Felder werden für Ergänzungen frei gehalten, die bei künftigen Überarbeitungen dieses Standards aufgenommen werden. Vorerst ist keines dieser Felder zu verwenden. Falls eines dieser Felder dennoch erscheinen sollte, so ist es zu ignorieren.

7.1.15. Feld 13.020: Comment (COM)

Dieses optionale Feld kann zur Eingabe von Bemerkungen oder anderer ASCII-Text-Informationen benutzt werden, die das Spuren-Bildmaterial begleiten.

7.1.16. Felder 13.021-13.199: Reserved for future definition (RSV)

Diese Felder werden für Ergänzungen frei gehalten, die bei künftigen Überarbeitungen dieses Standards aufgenommen werden. Vorerst ist keines dieser Felder zu verwenden. Falls eines dieser Felder auftreten sollte, so ist es zu ignorieren.

7.1.17. Felder 13.200-13.998: User-defined fields (UDF)

Diese vom Benutzer definierbaren Felder werden für künftige Zwecke benutzt werden. Ihr Umfang und Inhalt werden vom Benutzer definiert und müssen den Anforderungen der empfangenden Stelle entsprechen. Im Falle ihrer Verwendung enthalten sie ASCII-Text-Informationen.

7.1.18. Feld 13.999: Image data (DAT)

Dieses Feld enthält alle Daten eines gespeicherten Handflächenabdruckbildes. Dem Feld wird stets die Feldnummer „999“ zugewiesen, und es muss das letzte physische Feld des Datensatzes sein. Beispielsweise folgen auf „13.999:“ die Bilddaten in binärer Darstellung.

Jedes Pixel der unkomprimierten Graustufendaten wird normalerweise in 8 Bits umgesetzt (256 Graustufen), die in einem einzigen Byte enthalten sind. Ist der Wert im „BPX Field 13.012“ größer oder kleiner als „8“, so ändert sich die Anzahl der Bytes, die einen Pixel enthalten. Falls komprimiert wird, so muss die Kompression der Pixeldaten entsprechend der im „CGA Field“ festgelegten Kompressionstechnik erfolgen.

7.2. *Ende von Typ-13 Spuren-Bilddatei mit variabler Auflösung (End of Type-13 variable-resolution latent image record)*

Um Kohärenz zu gewährleisten, wird ein „FS“-Trennzeichen unmittelbar nach dem letzten Daten-Byte des Feldes 13.999 eingefügt, um dieses vom nächsten logischen Datensatz abzutrennen. Dieses Trennzeichen ist Bestandteil des Längenfelds des Typ-13-Datensatzes.

8. ***Typ-15 Handflächenabdruck-Bilddatei mit variabler Auflösung (Type-15 variable-resolution palmprint image record)***

Der logische Datensatz Typ-15 mit nummerierten Feldern enthält Handflächenabdruck-Bilddaten und dient dazu, solche Daten zusammen mit vorgegebenen und benutzerdefinierten textbasierten Informationsfeldern, die für das digitalisierte Bildmaterial von Bedeutung sind, zu übermitteln. Angaben über die verwendete Scanner-Auflösung, die Bildgröße und andere Parameter oder Bemerkungen, die zur Verarbeitung des Bildes erforderlich sind, werden als nummerierte Felder in den Datensatz eingestellt. An andere Behörden übermittelte Handflächenabdruckbilder werden von den empfangenden Stellen verarbeitet, um die gewünschten Merkmalsinformationen zu extrahieren, die für die Ermittlung einer Übereinstimmung erforderlich sind.

Die Aufnahme der Bilddaten erfolgt unmittelbar bei der erkennungsdienstlich zu behandelnden Person anhand eines Livescanners oder eines Handflächenabdruckblatts oder eines anderen Aufnahmemediums, welches die Handflächenabdrücke der Person enthält.

Jede Methode zur Aufnahme der Handflächenbilder sollte die Möglichkeit bieten, einen Satz von Bildern von jeder Hand zu speichern. Dieser Satz umfasst den Abdruck der beim Schreiben aufliegenden Handflächenkante (writer's palm) als Einzelscan sowie den gesamten Handflächenbereich vom Handgelenk bis zu den Fingerspitzen in der Form von 1 oder 2 eingescannten Bildern. Falls 2 Bilder zur Darstellung der gesamten Handfläche verwendet werden, so erstreckt sich das untere Bild vom Handgelenk bis zum Ende des Zwischenfingerbereichs (drittes Fingergelenk) und umfasst den Thenar- und den Hypothenarbereich der Handfläche. Das obere Bild erstreckt sich vom oberen Fingerwurzelbereich bis zu den Fingerspitzen. Hierdurch wird eine ausreichende Überlappung zwischen den beiden sich im Fingerwurzelbereich überschneidenden Bildern gewährleistet. Durch Abgleich der Papillarlinien und der Details in den überlappenden Handflächenbereichen erlangt der Prüfer die Gewissheit, dass beide Bilder von derselben Handfläche stammen.

Da eine Handflächenabdruck-Transaktion verschiedenen Zwecken dienen kann, darf sie eine oder mehrere einmalige Bildbereiche enthalten, die von der Handfläche oder Hand aufgenommen wurden. Ein vollständiger Satz von Handflächenabdrücken einer Person enthält in der Regel die Handkante (writer's palm) und einen vollständigen Abdruck jeder einzelnen Handfläche auf 1 oder 2 Bildern. Da eine logische Bilddatei mit nummerierten Feldern nur ein binäres Feld enthalten darf, sind für jeden Handkantenabdruck ein einziger Typ-15-Datensatz und für jeden vollständigen Handflächenabdruck 1 oder 2 Typ-15-Datensätze vorgeschrieben. Somit sind 4 bis 6 Typ-15-Datensätze erforderlich, um die Handflächenabdrücke einer Person in einer gewöhnlichen Handfächenabdruck-Transaktion darzustellen.

8.1. *Felder für den Typ-15 logischen Datensatz (Fields for the Type-15 logical record)*

In den folgenden Absätzen werden die Daten beschrieben, die in jedem einzelnen der Felder des Typ-15 logischen Datensatzes enthalten sind.

Innerhalb eines Typ-15 logischen Datensatzes sind nummerierte Felder für Einträge vorgesehen. Es ist notwendig, dass die Reihenfolge für die ersten beiden Felder des Datensatzes eingehalten wird und dass das Feld mit den Bilddaten das letzte physische Feld im Datensatz bildet. Zu jedem Feld des Typ-15-Datensatzes enthält Tabelle 8 folgende Angaben: Bedingungscode (condition code) mit dem Wert „M“ (mandatory — obligatorisch) oder „O“ (optional — fakultativ), Feldnummer (field number), Zeichensatz (character type), Feldgröße (field size) und quantitative Begrenzung der Vorkommnisse (occurrance limits). Die letzte Spalte gibt anhand einer 3-stelligen Feldnummer die maximale Feldgröße in Bytes an. Wenn mehr Stellen für die Feldnummer verwendet werden, steigt auch die maximale Bytezahl. Die beiden Einträge unter „field size per occurrence“ umfassen alle im Feld verwendeten Trennzeichen. Unter „maximum byte count“ fallen die Feldnummer, die Information und alle Trennzeichen einschließlich des „GS“-Trennzeichens.

8.1.1. Feld 15.001: Logical record length (LEN)

Dieses obligatorische ASCII-Feld gibt die Gesamtzahl der Bytes in dem Typ-15-Datensatz an. Feld 15.001 enthält die Länge des Datensatzes einschließlich aller Zeichen in allen Feldern des Datensatzes sowie die Informationstrennzeichen.

8.1.2. Feld 15.002: Image Designation Character (IDC)

Mit diesem obligatorischen ASCII-Feld wird das im Datensatz enthaltene Handflächenabdruckbild identifiziert. Dieses Feld entspricht dem IDC im Feld (CNT) des Typ-1-Datensatzes.

8.1.3. Feld 15.003: Impression type (IMP)

Dieses obligatorische 1-Byte-Feld beschreibt, auf welche Weise die Bildinformationen zum Handflächenabdruck gewonnen wurden. Der geeignete Code aus der Tabelle 9 wird zur Kennzeichnung des Abdrucktyps in dieses Feld eingegeben.

8.1.4. Feld 15.004: Source agency/ORI (SRC)

Dieses obligatorische ASCII-Feld bezeichnet die Behörde oder Organisation, die das im Datensatz enthaltene Handflächenbild ursprünglich erfasst hat. In der Regel enthält dieses Feld die Absenderkennung (Originating Agency Identifier — ORI) der Stelle, die das Bild erfasst hat. Das Feld besteht aus 2 Datenelementen, die das Format CC/agency haben.

Das erste Datenelement enthält den Interpol-Ländercode, der sich aus 2 alphanumerischen Zeichen zusammensetzt. Das zweite Datenelement, „agency“, dient der freitextlichen Bezeichnung der betreffenden Stellen mit maximal 32 alphanumerischen Zeichen.

8.1.5. Feld 15.005: Palmprint capture date (PCD)

Dieses obligatorische ASCII-Feld gibt das Datum an, an welchem der im Datensatz enthaltene Handflächenabdruck erfasst wurde. Das Datum besteht aus 8 Zeichen im Format CCYYMMDD. Die Zeichen CCYY geben das Jahr der Bilderfassung, die Zeichen MM die Zehner- und Einer-Stelle des Monats und die Zeichen DD die Zehner- und Einer-Stelle des Tags des entsprechenden Monats an. 20000229 bedeutet beispielsweise 29. Februar 2000. Das vollständige Datum muss ein gültiges Datum ergeben.

8.1.6. Feld 15.006: Horizontal line length (HLL)

Dieses obligatorische ASCII-Feld gibt die Pixelzahl einer einzelnen horizontalen Zeilenlänge des übertragenen Bildes an.

8.1.7. Feld 15.007: Vertical line length (VLL)

Dieses obligatorische ASCII-Feld gibt die Zahl der im übertragenen Bild enthaltenen horizontalen Zeilen an.

8.1.8. Feld 15.008: Scale units (SLC)

Dieses obligatorische ASCII-Feld nennt die Maßeinheiten für die Angabe der Bildabtastfrequenz (Pixeldichte). Eine „1“ in diesem Feld bedeutet Pixel/Inch, eine „2“ steht für Pixel/cm. Eine „0“ in diesem Feld bedeutet, dass keine Maßeinheit vorgegeben wurde. In diesem Fall liefert der Quotient aus HPS/VPS das Seitenverhältnis.

8.1.9. Feld 15.009: Horizontal pixel scale (HPS)

Dieses obligatorische ASCII-Feld gibt die ganzzahlige Pixeldichte in horizontaler Richtung an, wenn im SLC-Feld eine „1“ oder eine „2“ steht. Andernfalls gibt es die horizontale Komponente des Pixel-Seitenverhältnisses an.

8.1.10. Feld 15.010: Vertical pixel scale (VPS)

Dieses obligatorische ASCII-Feld gibt die ganzzahlige Pixeldichte in vertikaler Richtung an, wenn im SLC-Feld eine „1“ oder eine „2“ steht. Andernfalls gibt es die vertikale Komponente des Pixel-Seitenverhältnisses an.

Tabelle 8: Typ-15-Datensatzlayout für Handflächenabdrucke mit variabler Auflösung (Type-15 variable-resolution palmprint record layout)

Ident	Cond. code	Field number	Field name	Char type	Field size per occurrence		Occur count		Max. byte count
					min.	max.	min.	max.	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
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	—

Tabelle 9: Art des Handflächenabdrucks (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. Feld 15.011: Compression algorithm (CGA)

Dieses obligatorische ASCII-Feld bestimmt den Algorithmus für die Komprimierung von Graustufenbildern. Der Eintrag „NONE“ in diesem Feld bedeutet, dass die in diesem Datensatz enthaltenen Daten nicht komprimiert wurden. Im Hinblick auf diejenigen Bilder, die zu komprimieren sind, gibt dieses Feld die bevorzugte Methode für die Komprimierung von Zehnfingerabdruckblättern an. Die gültigen Komprimierungscodes sind in Anlage 7 definiert.

8.1.12. Feld 15.012: Bits per pixel (BPX)

Dieses obligatorische ASCII-Feld gibt die Anzahl der Bits an, die zur Darstellung eines Pixels verwendet werden. Dieses Feld enthält den Wert „8“ für normale Graustufenwerte von „0“ bis „255“. Jeglicher Wert über oder unter „8“ in diesem Feld verweist auf einen Graustufenpixel mit jeweils erhöhter bzw. verringerter Präzision.

Tabelle 10: Handflächencodes, -zonen und -größen (Palm Codes, Areas and Sizes)

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

8.1.13. Feld 15.013: Palmprint position (PLP)

Dieses obligatorische nummerierte Feld beschreibt die Position der Handfläche im entsprechenden Handflächenabdruckbild. Der Dezimalcodewert, der der bekannten oder wahrscheinlichsten Handfächenabdruckposition entspricht, wird der Tabelle 10 entnommen und als 2-stelliges ASCII-Unterfeld eingegeben. Die Tabelle 10 listet zudem die größtmöglichen Bildbereiche und Dimensionen für jede einzelne der möglichen Handflächenabdruckpositionen auf.

8.1.14. Felder 15.014-15.019: Reserved for future definition (RSV)

Diese Felder werden für Ergänzungen frei gehalten, die bei künftigen Überarbeitungen dieses Standards aufgenommen werden. Vorerst ist keines dieser Felder zu verwenden. Falls eines dieser Felder dennoch erscheinen sollte, so ist es zu ignorieren.

8.1.15. Feld 15.020: Comment (COM)

Dieses fakultative Feld kann zur Eingabe von Bemerkungen oder anderer ASCII-Text-Informationen benutzt werden, die Bildmaterial zum Handflächenabdruck begleiten.

8.1.16. Felder 15.021-15.199: Reserved for future definition (RSV)

Diese Felder werden für Ergänzungen frei gehalten, die bei künftigen Überarbeitungen dieses Standards aufgenommen werden. Vorerst ist keines dieser Felder zu verwenden. Falls eines dieser Felder auftreten sollte, so ist es zu ignorieren.

8.1.17. Felder 15.200-15.998: User-defined fields (UDF)

Diese vom Benutzer definierbaren Felder werden für künftige Zwecke benutzt werden. Ihr Umfang und Inhalt werden vom Benutzer definiert und müssen den Anforderungen der empfangenden Stelle entsprechen. Im Falle ihrer Verwendung enthalten sie ASCII-Text-Informationen.

8.1.18. Feld 15.999: Image data (DAT)

Dieses Feld enthält alle Daten eines aufgenommenen Handflächenabdruckbildes. Dem Feld wird stets die Feldnummer „999“ zugewiesen, und es muss das letzte physische Feld des Datensatzes sein. Beispielsweise folgen auf „15.999:“ die Bilddaten in binärer Darstellung. Jedes Pixel der unkomprimierten Graustufendaten wird normalerweise in 8 Bits umgesetzt (256 Graustufen), die in einem einzigen Byte enthalten sind. Ist der Wert im „BPX Field 15.012“ größer oder kleiner als „8“, so ändert sich die Anzahl der Bytes, die einen Pixel enthalten. Falls komprimiert wird, so muss die Kompression der Pixeldaten entsprechend der im „CGA Field“ festgelegten Komprimierungstechnik erfolgen.

8.2. *Ende von Typ-15 Handflächenabdruck-Bilddatei mit variabler Auflösung (End of Type-15 variable-resolution palmprint image record)*

Um Kohärenz zu gewährleisten, wird ein „FS"-Trennzeichen unmittelbar nach dem letzten Byte der Bilddaten des Feldes 15.999 eingefügt, um dieses vom nächsten Datensatz abzutrennen. Dieses Trennzeichen ist Bestandteil des Längenfelds des Typ-15-Datensatzes.

8.3. *Zusätzliche Typ-15 Handflächenabdruck-Bilddatei mit variabler Auflösung (Additional Type-15 variable-resolution palmprint image records)*

Zusätzliche Typ-15-Datensätze können in die Datei aufgenommen werden. Jedes zusätzliche Handflächenabdruckbild erfordert einen vollständigen Typ-15-Datensatz nebst „FS"-Trennzeichen.

Tabelle 11: Höchstzahl der pro Übertragung für eine Überprüfung akzeptierten Kandidaten

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

Art der Suche:

TP/TP: Zehnfingerabdruck gegen Zehnfingerabdruck (ten-print against ten-print)

LT/TP: Fingerabdruckspur gegen Zehnfingerabdruck (fingerprint latent against ten-print)

LP/PP: Handflächenabdruckspur gegen Handflächenabdruck (palmprint latent against palmprint)

TP/UL: Zehnfingerabdruck gegen offene Fingerabdruckspur (ten-print against unsolved fingerprint latent)

LT/UL: Fingerabdruckspur gegen offene Fingerabdruckspur (fingerprint latent against unsolved fingerprint latent)

PP/ULP: Handflächenabdruck gegen offene Handflächenabdruckspur (palmprint against unsolved palmprint latent)

LP/ULP: Handflächenabdruckspur gegen offene Handflächenabdruckspur (palmprint latent against unsolved palmprint latent)

9. ***Anlagen zu Kapitel 2 (Austausch daktyloskopischer Daten)***

9.1. *Anlage 1 — Codes der ASCII-Trennzeichen*

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]) Diese Position entspricht dem ASCII-Standard.

9.2. *Anlage 2 — Berechnung des alphanumerischen Kontrollzeichens (Check Character)*

Für TCN und TCR (Felder 1.09 und 1.10):

Die Nummer, die dem Kontrollzeichen entspricht, wird anhand folgender Formel generiert:

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

Die numerischen Werte YY und SSSSSSSS bezeichnen jeweils die beiden letzten Ziffern des Jahres und die Seriennummer.

Das Kontrollzeichen wird anschließend anhand der nachstehenden Bezugstabelle generiert.

Für CRO (Feld 2.010):

Die Nummer, die dem Kontrollzeichen entspricht, wird anhand folgender Formel generiert:

(YY * 10^6 + NNNNNN) Modulo 23

Die numerischen Werte YY und SSSSSSSS bezeichnen jeweils die beiden letzten Ziffern des Jahres und die Seriennummer.

Das Kontrollzeichen wird anschließend anhand der nachstehenden Bezugstabelle generiert.

Bezugstabelle für das Kontrollzeichen

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

9.3. *Anlage 3 — Zeichencodes*

7-Bit-ANSI-Code für den Informationsaustausch

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	»	#	$	%	&	‘
40	(	)	*	+	,	—	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

9.4. *Anlage 4 — Transaktionsübersicht*

Typ-1-Datensatz (obligatorisch)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1001	Logical Record Length	M	M	M
VER	1002	Version Number	M	M	M
CNT	1003	File Content	M	M	M

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
TOT	1004	Type of Transaction	M	M	M
DAT	1005	Date	M	M	M
PRY	1006	Priority	M	M	M
DAI	1007	Destination Agency	M	M	M
ORI	1008	Originating Agency	M	M	M
TCN	1009	Transaction Control Number	M	M	M
TCR	1010	Transaction Control Reference	C	M	M
NSR	1011	Native Scanning Resolution	M	M	M
NTR	1012	Nominal Transmitting Resolution	M	M	M
DOM	1013	Domain name	M	M	M
GMT	1014	Greenwich mean time	M	M	M

Schlüssel:

O = Optional (fakultativ); M = Mandatory (obligatorisch); C = Conditional (bedingt), falls die Transaktion eine Antwort auf die anfragende Stelle darstellt.

Typ-2-Datensatz (obligatorisch)

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	—	—

Schlüssel:

O = Optional (fakultativ); M = Mandatory (obligatorisch); C = Conditional (bedingt), falls Daten vorhanden sind.

* = falls die Übermittlung der Daten nach nationalem Recht erfolgt (fällt nicht unter den Beschluss 2008/615/JI)

9.5. *Anlage 5 — Typ-1-Datensatz: Definitionen*

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

In der Spalte „Condition“: O = Optional (fakultativ); M = Mandatory (obligatorisch); C = Conditional (bedingt).

In der Spalte „Character Type“: A = Alphanumerisch; N = Numerisch; B = Binär;

1* = zugelassene Zeichen zur Angabe des Namens der Stelle [„0..9“, „A..Z“, „a..z“, „_“, „.“, „,“, „—“].

9.6. *Anlage 6 — Typ-2-Datensatz: Definitionen*

Tabelle A.6.1: CPS- und PMS-Transaktionen

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

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

Tabelle A.6.2: SRE-Transaktion

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

Tabelle A.6.3: ERR-Transaktion

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

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

Tabelle A.6.4: MPS- und MMS-Transaktion

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}

In der Spalte „Condition“: O = Optional (fakultativ); M = Mandatory (obligatorisch); C = Conditional (bedingt).

In der Spalte „Character Type“: A = Alphanumerisch; N = Numerisch; B = Binär;

1* = zugelassene Zeichen sind [„0..9“, „A..Z“, „a..z“, „_“, „.“, „,“, „—“, „‚“].

9.7. *Anlage 7 — Graustufenkomprimierungscodes*

Komprimierungscodes

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

9.8. *Anlage 8 — Mailspezifikation*

Zur Verbesserung der internen Arbeitsabläufe ist bei PRUEM-Transaktionen im Betreff-Feld der Mail der Ländercode (CC) des Absender-Mitgliedstaats und die Art der Transaktion (TOT-Feld 1.004) anzugeben.

Format: CC/*type of transaction*

Beispiel: „DE/CPS“

Der Mail-Body kann leer sein.

KAPITEL 3: **Austausch von Daten aus den Fahrzeugregistern**

1. ***Einheitlicher Datensatz für den automatisierten Abruf von Daten aus den Fahrzeugregistern***

1.1. *Begriffsbestimmungen*

Für obligatorische und optionale Datenelemente gemäß Artikel 16 Absatz 4 gelten die folgenden Begriffsbestimmungen:

Obligatorisch (M = Mandatory):

Das Datenelement ist zu übermitteln, wenn Angaben im nationalen Fahrzeugregister eines Mitgliedstaats vorliegen. Daher besteht die Pflicht zum Austausch der Angaben, wenn sie verfügbar sind.

Optional (O):

Das Datenelement kann übermittelt werden, wenn die Angaben im nationalen Fahrzeugregister eines Mitgliedstaats vorliegen. Daher besteht keine Pflicht zum Austausch der Angaben, selbst wenn sie verfügbar sind.

Jedes Element des Datensatzes, das in Bezug auf den Beschluss 2008/615/JI als besonders wichtig hervorzuheben ist, wird mit „Y" gekennzeichnet.

1.2. *Abruf von Fahrzeug-/Eigentümer-/Halterdaten*

1.2.1. Abrufkriterien

Es gibt zwei Möglichkeiten für den Datenabruf der im nächsten Absatz beschriebenen Informationen:

— Abruf mit Fahrzeug-Identifizierungsnummer (FIN), Stichtag und Uhrzeit (optional);

— Abruf mit Registrierungsnummer (Kennzeichen), Fahrzeug-Identifizierungsnummer (FIN) (optional), Stichtag und Uhrzeit (optional).

Anhand dieser Abrufkriterien können Angaben zu einem Fahrzeug, bisweilen auch zu mehreren Fahrzeugen, gefunden werden. Finden sich Angaben nur zu einem Fahrzeug, so werden alle Datenelemente in einer Auskunft ausgegeben. Finden sich Angaben zu mehr als einem Fahrzeug, so kann der die Anfrage empfangende Mitgliedstaat (z. B. aus Datenschutz- oder Kapazitätsgründen) entscheiden, welche Datenelemente in die Auskunft aufgenommen werden, d. h. entweder alle Datenelemente oder nur die Datenelemente, die für die Abrufverfeinerung notwendig sind.

Die für die Abrufverfeinerung notwendigen Datenelemente sind in Nummer 1.2.2.1 wiedergegeben. In Nummer 1.2.2.2 ist der vollständige Auskunftsdatensatz beschrieben.

Abrufe mit Fahrzeug-Identifizierungsnummer, Stichtag und Uhrzeit können an einen oder alle beteiligten Mitgliedstaaten gerichtet werden.

Abrufe mit Registrierungsnummer (Kennzeichen), Stichtag und Uhrzeit sind an einen bestimmten Mitgliedstaat zu richten.

Üblicherweise werden für den Abruf das aktuelle Datum und die aktuelle Uhrzeit verwendet, doch kann ein Abruf auch auf zurückliegende Stichtage und Uhrzeiten bezogen werden. Wird ein Abruf mit in der Vergangenheit liegenden Stichtagen und Uhrzeiten durchgeführt und finden sich im Register des betreffenden Mitgliedstaats keine „historischen" Angaben, weil solche Daten nicht gespeichert werden, können die aktuellen Angaben — versehen mit einem Vermerk, dass es sich um aktuelle Angaben handelt — in die Auskunft aufgenommen werden.

1.2.2. Datensatz

1.2.2.1. Notwendige Datenelemente für die Abrufverfeinerung

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

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

(1) M = mandatory when available in national register, O = optional.
(2) All the attributes specifically allocated by the Member States are indicated with Y.
(3) Harmonised document abbreviation, see Council Directive 1999/37/EC of 29.4.1999.

1.2.2.2. Vollständiger Datensatz

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

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

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

[1] M = mandatory when available in national register, O = optional.
[2] Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999.
[3] In Luxembourg two separate vehicle registration document ID's are used.

2. ***Datensicherheit***

2.1. *Allgemeines*

Die Eucaris-Softwareanwendung ermöglicht eine sichere Verbindung zu den anderen Mitgliedstaaten und die Kommunikation mit den Back-End Legacy-Systemen der Mitgliedstaaten unter Nutzung von XML. Die Mitgliedstaaten tauschen Nachrichten durch direkte Übermittlung an den Empfänger aus. Das Datenzentrum eines Mitgliedstaats ist an das TESTA- Kommunikationsnetzwerk der EU angeschlossen.

Die über das Netzwerk übertragenen XML-Nachrichten sind verschlüsselt. Als Verschlüsselungsverfahren für diese Nachrichten dient SSL. Die an das Back-End-System übertragenen Nachrichten sind XML-Nachrichten in Klartext, da sich die Verbindung zwischen der Anwendung und dem Back-End-System in einer geschützten Umgebung befindet.

Es ist eine Client-Anwendung vorhanden, die von einem Mitgliedstaat für Abfragen im eigenen nationalen Register oder in den Registern anderer Mitgliedstaaten verwendet werden kann. Clients werden mittels Nutzer-ID/Passwort oder Client-Zertifikat identifiziert. Die Verbindung zu einem Nutzer kann verschlüsselt werden, doch fällt dies in die Zuständigkeit jedes einzelnen Mitgliedstaats.

2.2. *Sicherheitsmerkmale in Bezug auf den Nachrichtenaustausch*

Das Sicherheitskonzept kombiniert HTTPS- und XML-Signatur. Bei dieser Variante wird die XML-Signatur verwendet, um alle an den Server übertragenen Nachrichten zu signieren; mit ihr kann der Absender durch Prüfung der Signatur authentisiert werden. 1-seitiges (1-sided) SSL (nur Serverzertifikat) wird zum Schutz der Vertraulichkeit und Integrität der Nachricht bei der Übertragung und zur Abwehr von Lösch-, Wiedereinspiel- oder Einfügungsattacken verwendet. Anstelle einer maßgeschneiderten Softwareentwicklung zur Implementierung von 2-seitigem (2-sided) SSL wird die XML-Signatur eingesetzt. Die Nutzung der XML-Signatur ist näher an der Web Services Roadmap als das 2-seitige SSL und deshalb strategisch vorteilhafter.

Die XML-Signatur kann auf vielerlei Weise implementiert werden, doch die ausgewählte Methode ist ihre Verwendung als Bestandteil der Web Services Security (WSS). WSS gibt im Einzelnen vor, wie die XML-Signatur einzusetzen ist. Da WSS auf dem SOAP-Standard basiert, ist es logisch, dass am SOAP-Standard so weit wie möglich festgehalten werden sollte.

2.3. *Sicherheitsmerkmale ohne Bezug zum Nachrichtenaustausch*

2.3.1. Authentisierung von Nutzern

Die Nutzer der Eucaris-Web-Anwendung authentisieren sich durch einen Nutzernamen und ein Passwort. Da die übliche Windows-Authentisierung genutzt wird, können die Mitgliedstaaten bei Bedarf den Authentisierungsgrad durch Einsatz von Client-Zertifikaten erhöhen.

2.3.2. Nutzerrollen (user roles)

Die Eucaris-Softwareanwendung unterstützt verschiedene Nutzerrollen. Zu jeder Gruppe von Diensten gehört eine eigene Autorisierung. Beispielsweise können Nutzer, die (ausschließlich) Zugriff auf die Funktionalitäten nach dem Eucaris-Vertrag haben, die Funktionalitäten des Prümer Vertrags nicht nutzen. Administratordienste sind von den normalen Endnutzerrollen getrennt.

2.3.3. Protokollierung und Überwachung (tracing) des Nachrichtenaustauschs

Die Protokollierung wird durch die Eucaris-Softwareanwendung unterstützt. Durch eine Administratorfunktion kann der nationale Administrator entscheiden, welche Nachrichten protokolliert werden, z. B. Anfragen von Endnutzern, aus anderen Mitgliedstaaten eingehende Anfragen, aus den nationalen Registern bereitgestellte Angaben usw.

Die Anwendung kann so konfiguriert werden, dass für die Protokollierung entweder eine interne oder eine externe (Oracle) Datenbank zum Einsatz kommt. Die Entscheidung darüber, welche Nachrichten protokolliert werden sollen, hängt eindeutig davon ab, welche Protokollierungsmöglichkeiten es sonst noch in den Legacy-Systemen und den angeschlossenen Client-Anwendungen gibt.

Im Kopf jeder Nachricht sind der anfragende Mitgliedstaat, die anfragende Stelle in diesem Mitgliedstaat und der betreffende Nutzer sowie der Grund der Anfrage anzugeben.

Durch die kombinierte Protokollierung im anfragenden und im antwortenden Mitgliedstaat ist eine vollständige Nachvollziehbarkeit jedes Nachrichtenaustauschs (z. B. auf Antrag eines betroffenen Bürgers) möglich.

Die Protokollierung wird über das Eucaris-Web-Client (Menu Administration, Logging configuration) konfiguriert. Die Protokollierfunktionalität wird vom Kernsystem bereitgestellt. Ist die Protokollierung aktiviert, so wird die komplette Nachricht (Kopf und Text) in einem Protokollarchiv gespeichert. Die Protokollierungsebene kann je nach vordefiniertem Dienst und Art der Nachricht, die das Kernsystem durchläuft, gewählt werden.

Protokollierungsebenen

Folgende Protokollierungsebenen sind möglich:

Privat — Nachricht wird protokolliert: Die Protokollierung ist NICHT vom Auszugsprotokolldienst (extract logging service) abrufbar, sondern nur auf nationaler Ebene für Audits und die Behebung von Problemen verwendbar.

Keine — Nachricht wird in keinem Fall protokolliert.

Arten von Nachrichten

Der Informationsaustausch zwischen Mitgliedstaaten beinhaltet verschiedene Nachrichten, die in der nachstehenden Abbildung schematisch dargestellt sind.

Folgende Nachrichtenarten (in der Abbildung beziehen sie sich auf das Eucaris-Kernsystem eines Mitgliedstaats X) sind möglich:

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

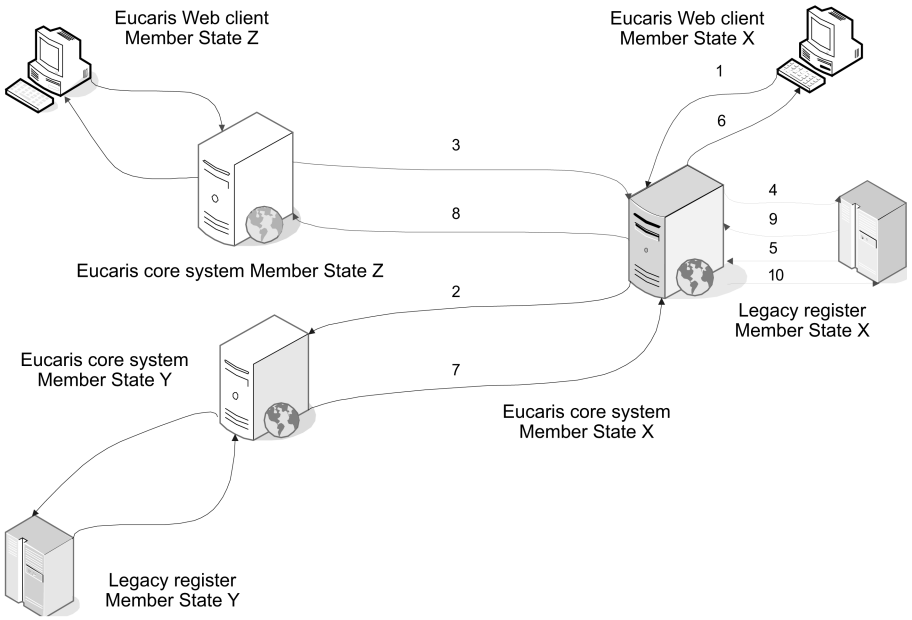
Folgende Varianten des Informationsaustauschs sind in der Abbildung dargestellt:

— Auskunftsersuchen von Mitgliedstaat X an Mitgliedstaat Y — blaue Pfeile. Abruf und Rückmeldung bestehen aus dem Nachrichtentyp 1, 2, 7 bzw. 6.

— Auskunftsersuchen von Mitgliedstaat Z an Mitgliedstaat X — rote Pfeile. Abruf und Rückmeldung bestehen aus dem Nachrichtentyp 3, 4, 9 bzw. 8.

— Auskunftsersuchen vom Legacy-Register an sein Kernsystem (diese Kommunikation bezieht auch Anfragen von Custom-Clients hinter dem Legacy-Register mit ein) — grüne Pfeile. Diese Anfragekategorie setzt sich aus den Nachrichtentypen 5 und 10 zusammen.

Abbildung: Nachrichtentypen für die Protokollierung



2.3.4. Hardware-Sicherheitsmodul

Ein Hardware-Sicherheitsmodul kommt nicht zum Einsatz.

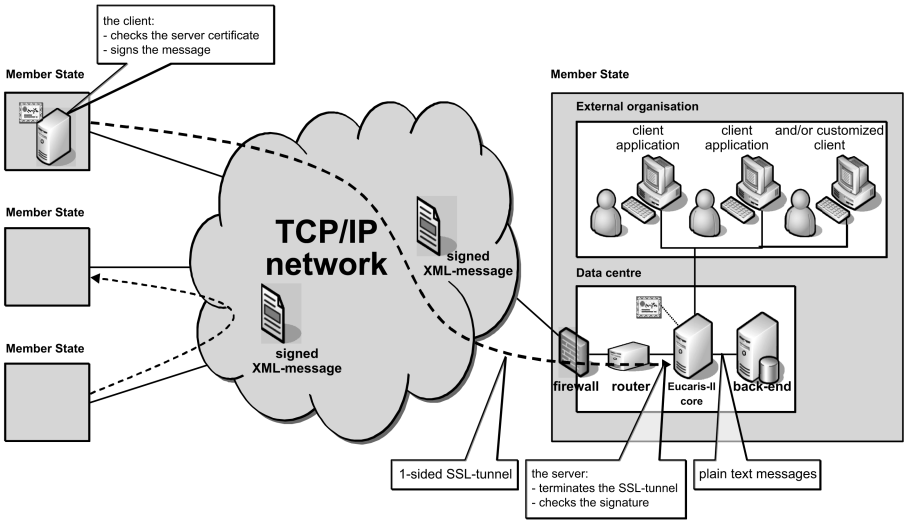
Hardware-Sicherheitsmodule (HSM) bieten einen guten Schutz für Schlüssel, die zum Signieren von Nachrichten und zur Identifizierung von Diensten/Servern verwendet werden. Sie heben das insgesamt vorhandene Sicherheitsniveau weiter an, sind aber teuer in der Anschaffung und Wartung; zudem bestehen keine Anforderungen für ein HSM nach Standard FIPS 140-2 Level 2 oder Level 3. Da ein geschlossenes Netzwerk verwendet wird, das wirksam vor Bedrohungen schützt, wurde entschieden, nicht von Anfang an ein HSM einzusetzen. Sollte es — z. B. für Akkreditierungen — notwendig werden, kann es nachträglich in die Architektur integriert werden.

3. *Technische Bedingungen für den Datenaustausch*

3.1. *Beschreibung der Eucaris-Anwendung*

3.1.1. Allgemeines

Durch die Eucaris-Anwendung werden alle beteiligten Mitgliedstaaten in einem vermaschten Netz zusammengeschaltet, in dem jeder Mitgliedstaat direkt mit dem anderen kommuniziert. Für die Kommunikation ist keine zentrale Komponente erforderlich. Die Eucaris-Softwareanwendung erlaubt eine sichere Verbindung zu den anderen Mitgliedstaaten und die Kommunikation mit den Back-End Legacy-Systemen der Mitgliedstaaten unter Nutzung von XML. Die nachstehende Abbildung zeigt diese Architektur.



Die Mitgliedstaaten tauschen Nachrichten durch direkte Übermittlung an den Empfänger aus. Das Datenzentrum eines Mitgliedstaats ist an das für den Nachrichtenaustausch genutzte Netzwerk (TESTA) angeschlossen. Die Mitgliedstaaten erhalten Zugang zum TESTA-Netz über ihr nationales Portal (Gate). Die Verbindung zum Netz muss über eine Firewall laufen; ein Router wiederum verbindet die Eucaris-Anwendung mit der Firewall. In Abhängigkeit von der für den Schutz der Nachrichten gewählten Option wird ein Zertifikat entweder durch den Router oder durch die Eucaris-Anwendung verwendet.

Es ist eine Client-Anwendung vorhanden, die von einem Mitgliedstaat für Abfragen im eigenen nationalen Register oder in den Registern anderer Mitgliedstaaten verwendet werden kann. Sie wird mit Eucaris verbunden. Clients werden mittels Nutzer-ID/Passwort oder Client-Zertifikat identifiziert. Die Verbindung zu einem Nutzer in einer externen Stelle (z. B. Polizei) kann verschlüsselt werden, doch fällt dies in die Zuständigkeit jedes einzelnen Mitgliedstaats.

3.1.2. Anwendungsbereich des Systems

Der Anwendungsbereich des Eucaris-Systems ist auf Prozesse im Zusammenhang mit dem Informationsaustausch zwischen den Registerbehörden der Mitgliedstaaten und eine Basisdarstellung dieser Informationen beschränkt. Verfahren und automatisierte Prozesse, für die die Informationen verwendet werden sollen, fallen nicht in den Anwendungsbereich des Systems.

Die Mitgliedstaaten können entscheiden, ob sie die Eucaris-Client-Funktionalität nutzen oder sich ihre eigene Client-Anwendung individuell gestalten wollen. In der nachstehenden Tabelle wird dargelegt, welche Elemente des Eucaris-Systems obligatorisch bzw. vorgeschrieben sind und welche optional sind bzw. von den Mitgliedstaaten frei gewählt werden können.

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

[1] M = mandatory to use or to comply with; O = optional to use or to comply with.

3.2. *Funktionale/nicht funktionale Anforderungen*

3.2.1. Generische Funktionalität

In diesem Abschnitt werden die wichtigsten generischen Funktionen in allgemeiner Form beschrieben.

Nr.	Beschreibung
1.	Das System ermöglicht den Registerbehörden der Mitgliedstaaten einen interaktiven Austausch von Anfragen und Auskünften.
2.	Das System beinhaltet eine Client-Anwendung, die Endnutzern den Versand ihrer Anfragen ermöglicht und die die Antwort für die manuelle Verarbeitung ausgibt.
3.	Das System erleichtert den „Rundruf", mit dem Mitgliedstaaten Anfragen an alle anderen Mitgliedstaaten senden können. Die eingehenden Antworten werden von der Kernanwendung in einer einzigen Antwortnachricht zusammengefasst (diese Funktionalität wird als „Mehrländerabfrage" bezeichnet).
4.	Das System kann verschiedene Arten von Nachrichten bearbeiten. Nutzerrollen, Autorisierung, Routing, Signierung und Protokollierung sind allesamt als gesonderte Dienste definiert.
5.	Das System ermöglicht den Mitgliedstaaten den Austausch von Nachrichtenstapeln und Nachrichten, die eine große Anzahl von Anfragen oder Antworten enthalten. Diese Nachrichten werden asynchron bearbeitet.
6.	Das System stellt asynchrone Nachrichten in eine Warteschlange, wenn der Empfängermitgliedstaat vorübergehend nicht erreichbar ist, und gewährleistet die Zustellung, sobald er wieder zur Verfügung steht.
7.	Das System speichert eingehende asynchrone Nachrichten, bis sie verarbeitet werden können.
8.	Das System erlaubt den Zugriff nur auf Eucaris-Anwendungen anderer Mitgliedstaaten, nicht aber auf einzelne Stellen der anderen Mitgliedstaaten, d. h., jede Registerbehörde fungiert als einziges Gateway zwischen ihren nationalen Endnutzern und den entsprechenden Registerbehörden der anderen Mitgliedstaaten.
9.	Es besteht die Möglichkeit, Nutzer aus verschiedenen Mitgliedstaaten auf einem Eucaris-Server zu definieren und sie nach Maßgabe der Rechte dieses Mitgliedstaats zu autorisieren.
10.	Die Nachrichten enthalten Angaben zum anfragenden Mitgliedstaat, zur anfragenden Stelle sowie zum Endnutzer.
11.	Das System erleichtert die Protokollierung des Nachrichtenaustauschs zwischen den einzelnen Mitgliedstaaten sowie zwischen der Kernanwendung und den nationalen Registrierungssystemen.
12.	Das System überträgt einer Stelle oder einem Mitgliedstaat die Sekretariatsfunktion und erteilt ihr/ihm ausdrücklich die Berechtigung, protokollierte Angaben über Nachrichten, die an alle Mitgliedstaaten übermittelt bzw. von diesen empfangen wurden, für die Erstellung statistischer Berichte zusammenzutragen.
13.	Jeder Mitgliedstaat legt selbst fest, welche protokollierten Angaben dem Sekretariat zugänglich gemacht werden und welche „privaten" Charakter tragen.
14.	Das System ermöglicht den nationalen Administratoren jedes Mitgliedstaats, statistische Daten für den Eigenbedarf abzurufen.
15.	Das System erlaubt die Aufnahme neuer Mitgliedstaaten über einfache administrative Funktionen.

3.2.2 Benutzerfreundlichkeit

Nr.	Beschreibung
16.	Das System besitzt eine Schnittstelle für die automatisierte Verarbeitung von Nachrichten durch Back-End-/Legacy-Systeme und ermöglicht die Einbeziehung von (kundenspezifischen) Nutzerschnittstellen in diese Systeme.
17.	Das System ist leicht erlernbar, selbsterklärend und enthält Hilfetext.
18.	Zum System gehört eine Dokumentation, die den Mitgliedstaaten die Einbindung des Systems sowie den operationellen Betrieb und künftige Wartungsarbeiten ermöglicht (z. B. Handbücher, Bedienungsanleitungen, technische Unterlagen, Betriebsunterlagen usw.).
19.	Die Nutzerschnittstelle ist mehrsprachig ausgelegt und bietet dem Endnutzer die Möglichkeit zur Auswahl der von ihm bevorzugten Sprache.
20.	Die Nutzerschnittstelle ermöglicht es dem Administrator vor Ort, Bildschirmanzeigen und codierte Informationen in die von ihm bevorzugte Sprache zu übersetzen.

3.2.3. Zuverlässigkeit

Nr.	Beschreibung
21.	Das System soll robust und betriebssicher gestaltet sein und Anwenderfehler, Stromausfälle und andere Problemfälle ohne Schwierigkeiten bewältigen. Es muss möglich sein, das System ohne oder mit minimalem Datenverlust neu zu starten.
22.	Das System soll stabile und reproduzierbare Ergebnisse liefern.
23.	Das System ist so gestaltet, dass es zuverlässig funktioniert. Es soll den Betrieb mit einer Konfiguration ermöglichen, die eine 98 %ige Verfügbarkeit (durch Redundanz, Verwendung von Backup-Servern usw.) bei jeder bilateralen Kommunikation garantiert.
24.	Es sollte möglich sein, auch bei Ausfall einiger Komponenten einen Teil des Systems zu nutzen (wenn Mitgliedstaat C ausfällt, müssen die Mitgliedstaaten A und B noch miteinander kommunizieren können). Die Zahl der punktuellen Ausfälle in der Informationskette soll möglichst gering gehalten werden.
25.	Die Einsatzfähigkeit nach einem größeren Ausfall muss innerhalb eines Tages wiederhergestellt sein. Es muss möglich sein, die Ausfallzeit durch Inanspruchnahme von Fernbetreuung, beispielsweise durch einen zentralen Service-Desk, auf ein Mindestmaß zu reduzieren.

3.2.4. Leistungsfähigkeit

Nr.	Beschreibung
26.	Das System muss 7 Tage rund um die Uhr einsetzbar sein. Diese zeitliche Vorgabe (7 Tage rund um die Uhr) muss dann auch von den Legacy-Systemen der Mitgliedstaaten erfüllt werden.
27.	Das System muss unabhängig von laufenden Hintergrundprogrammen schnell auf Nutzeranfragen reagieren. Diese Vorgabe gilt auch für die Legacy-Systeme der Teilnehmer, damit eine akzeptable Ansprechzeit sichergestellt wird. Eine Gesamtantwortzeit von 10 Sekunden pro Einzelanfrage ist vertretbar.
28.	Das System ist als Multi-User-System so zu gestalten, dass Hintergrundprogramme laufen können, während der Nutzer Vordergrundprogramme ausführt.
29.	Das System ist skalierbar zu gestalten, um etwaige Steigerungen der Nachrichtenanzahl bewältigen zu können, wenn neue Funktionalitäten bzw. neue Stellen oder Mitgliedstaaten in das System aufgenommen werden.

3.2.5. Sicherheit

Nr.	Beschreibung
30.	Das System muss (z. B. in Bezug auf sein Sicherheitskonzept) für den Austausch von Nachrichten mit sensiblen personenbezogenen Daten (z. B. über Besitzer/Halter von Kraftfahrzeugen), die als „EU restricted“ eingestuft sind, geeignet sein.
31.	Das System ist so einzurichten, dass jeder unbefugte Zugriff auf Daten verhindert wird.
32.	Das System enthält ein Managementprogramm für Rechte und Befugnisse der nationalen Endnutzer.
33.	Die Mitgliedstaaten müssen in der Lage sein, die Identität des Absenders über die XML-Signatur (auf Ebene des Mitgliedstaats) zu prüfen.
34.	Die Mitgliedstaaten müssen anderen Mitgliedstaaten die ausdrückliche Genehmigung zum Abruf von Informationen erteilen.
35.	Das System beinhaltet auf Anwendungsebene ein umfassendes Sicherheits- und Verschlüsselungskonzept, das dem für solche Fälle angemessenen Sicherheitsniveau genügt. Vertraulichkeit und Integrität der Informationen sind durch Verwendung der XML-Signatur und verschlüsselte Übertragung mit SSL-Tunnel zu gewährleisten.
36.	Jeder Nachrichtenaustausch kann mittels Protokollierung nachvollzogen werden.
37.	Ein Schutz gegen Löschattacken (Löschung einer Nachricht durch einen Dritten) und gegen Wiedereinspiel- oder Einfügungsattacken (Wiedereinspielung oder Einfügung einer Nachricht durch einen Dritten) muss gegeben sein.
38.	Das System verwendet Zertifikate einer vertrauenswürdigen dritten Partei (Trusted Third Party — TTP).
39.	Das System kann mit den in den Mitgliedstaaten je nach Nachrichten- oder Dienstart verwendeten unterschiedlichen Zertifikaten arbeiten.

Nr.	Beschreibung
40.	Die Sicherheitsmaßnahmen auf Anwendungsebene sind ausreichend, so dass die Verwendung von nicht akkreditierten Netzwerken möglich ist.
41.	Das System erlaubt die Verwendung neuer Sicherheitstechniken wie der XML-Firewall.

3.2.6. Anpassungsfähigkeit

Nr.	Beschreibung
42.	Das System lässt sich durch Aufnahme neuer Nachrichtenarten und Funktionalitäten erweitern. Die Anpassungskosten sollen aufgrund der zentralen Entwicklung von Anwendungskomponenten möglichst gering sein.
43.	Es muss den Mitgliedstaaten möglich sein, neue Nachrichtenarten für den bilateralen Gebrauch zu definieren. Es ist nicht erforderlich, dass alle Mitgliedstaaten jede Nachrichtenart unterstützen.

3.2.7. Betreuung und Wartung

Nr.	Beschreibung
44.	Das System sieht Überwachungseinrichtungen für einen zentralen Service-Desk und/oder Operatoren bezüglich des Netzwerks und der Server in den verschiedenen Mitgliedstaaten vor.
45.	Das System sieht Einrichtungen zur Fernbetreuung durch einen zentralen Service-Desk vor.
46.	Das System sieht Einrichtungen zur Problemanalyse vor.
47.	Das System lässt sich auf neue Mitgliedstaaten erweitern.
48.	Die Anwendung kann durch Personal mit einem Minimum an IT-Kenntnissen und -Erfahrungen installiert werden. Die Installation sollte weitgehend automatisiert erfolgen.
49.	Das System bietet eine ständige Test- und Akzeptanzumgebung.
50.	Die jährlichen Kosten für Wartung und Betreuung sind durch Übernahme von Marktstandards und durch Einsatz einer solchen Anwendung, die nur wenig Betreuung durch einen zentralen Service-Desk erfordert, möglichst gering zu halten.

3.2.8. Konzeptionelle Vorgaben

Nr.	Beschreibung
51.	Konzeption und Dokumentation des Systems sind für einen langjährigen Betriebszeitraum ausgelegt.
52.	Das System ist so zu konzipieren, dass es vom Netzbetreiber unabhängig ist.
53.	Das System ist mit der in den Mitgliedstaaten verwendeten Hardware/Software kompatibel, in dem es mit deren Registrierungssystemen unter Nutzung von Web-Service-Technologien mit offenen Standards (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 usw.) kommuniziert.

3.2.9. Anwendbare Standards

Nr.	Beschreibung
54.	Das System erfüllt die Datenschutzvorschriften der Verordnung (EG) Nr. 45/2001 (Artikel 21, 22 und 23) sowie der Richtlinie 95/46/EG.
55.	Das System erfüllt die IDA-Standards.
56.	Das System unterstützt UTF8.

KAPITEL 4: **Bewertung**

1. ***Bewertungsverfahren gemäß Artikel 20 (Vorbereitung der in Artikel 25 Absatz 2 des Beschlusses 2008/615/JI genannten Beschlüsse)***

1.1. *Fragebogen*

Die zuständige Ratsarbeitsgruppe erstellt einen Fragebogen für jede Art von automatisiertem Datenaustausch gemäß Kapitel 2 des Beschlusses 2008/615/JI.

Geht ein Mitgliedstaat davon aus, dass er die Voraussetzungen für einen Austausch von Daten der jeweiligen Kategorie erfüllt, so beantwortet er die entsprechenden Fragen.

1.2. *Testlauf*

Im Hinblick auf die Auswertung des Fragebogens führt der Mitgliedstaat, der mit dem Datenaustausch beginnen möchte, zusammen mit einem oder mehreren anderen Mitgliedstaaten, die bereits am Datenaustausch im Rahmen des Ratsbeschlusses beteiligt sind, einen Testlauf durch. Der Testlauf erfolgt kurz vor oder kurz nach dem Bewertungsbesuch.

Die Bedingungen und Modalitäten für diesen Testlauf werden auf der Grundlage einer zuvor mit dem betreffenden Mitgliedstaat geschlossenen gesonderten Vereinbarung von der zuständigen Ratsarbeitsgruppe festgelegt. Die an dem Testlauf beteiligten Mitgliedstaaten regeln die praktischen Einzelheiten.

1.3. *Bewertungsbesuch*

Im Hinblick auf die Auswertung des Fragebogens wird ein Bewertungsbesuch in dem Mitgliedstaat durchgeführt, der mit dem Datenaustausch beginnen möchte.

Die Bedingungen und Modalitäten für diesen Bewertungsbesuch werden auf der Grundlage einer zuvor zwischen dem betreffenden Mitgliedstaat und dem Bewertungsteam geschlossenen gesonderten Vereinbarung von der zuständigen Ratsarbeitsgruppe festgelegt. Der betreffende Mitgliedstaat ermöglicht dem Bewertungsteam die Kontrolle des automatisierten Datenaustauschs in der bzw. den zu bewertenden Datenkategorien insbesondere durch Erstellung eines Besuchsprogramms, das dem Auftrag des Bewertungsteams Rechnung trägt.

Innerhalb eines Monats erarbeitet das Bewertungsteam einen Bericht über den Bewertungsbesuch und leitet ihn dem betreffenden Mitgliedstaat zur Stellungnahme zu. Gegebenenfalls wird der Bericht auf der Grundlage der Stellungnahme des Mitgliedstaats vom Bewertungsteam überarbeitet.

Das Bewertungsteam besteht aus maximal drei Experten, die von den am automatisierten Datenaustausch in der bzw. den zu bewertenden Datenkategorien beteiligten Mitgliedstaaten ernannt werden. Diese Experten müssen über Erfahrungen mit der betreffenden Datenkategorie verfügen, im Besitz ausreichender Sicherheitsermächtigungen für die Behandlung dieser Fragen sein und bereit sein, an mindestens einem Bewertungsbesuch in einem anderen Mitgliedstaat teilzunehmen. Die Kommission wird ersucht, sich dem Bewertungsteam als Beobachter anzuschließen.

Die Mitglieder des Bewertungsteams wahren die Vertraulichkeit der Informationen, von denen sie bei der Durchführung ihres Auftrags Kenntnis erhalten.

1.4. *Bericht an den Rat*

Dem Rat wird zur Vorbereitung seines Beschlusses gemäß Artikel 25 Absatz 2 des Beschlusses 2008/615/JI ein Gesamtbericht mit einer umfassenden Evaluierung der Ergebnisse der Fragebogen, des Bewertungsbesuchs und des Testlaufs vorgelegt.

2. ***Bewertungsverfahren gemäß Artikel 21***

2.1. *Statistiken und Bericht*

Jeder Mitgliedstaat stellt Statistiken zu den Ergebnissen des automatisierten Datenaustauschs auf. Das Statistikmodell wird von der zuständigen Ratsarbeitsgruppe erarbeitet, um die Vergleichbarkeit der Daten zu gewährleisten.

Diese Statistiken werden jährlich dem Generalsekretariat, das einen zusammenfassenden Überblick über das abgelaufene Jahr erstellt, sowie der Kommission zugeleitet.

Darüber hinaus werden die Mitgliedstaaten gebeten, regelmäßig, aber nicht häufiger als einmal pro Jahr weitere Angaben über die verwaltungsmäßige, technische und finanzielle Umsetzung des automatisierten Datenaustauschs vorzulegen, damit das Verfahren — wenn nötig — analysiert und verbessert werden kann. Anhand dieser Informationen wird ein Bericht für den Rat erstellt.

2.2. *Überarbeitung*

Der Rat wird das hier beschriebene Bewertungsverfahren binnen einer angemessenen Frist prüfen und erforderlichenfalls überarbeiten.

3. Treffen von Experten

Die Experten treffen im Rahmen der zuständigen Ratsarbeitsgruppe regelmäßig zur Vorbereitung und Durchführung der vorgenannten Bewertungsverfahren sowie zum Erfahrungsaustausch und zur Erörterung etwaiger Verbesserungen zusammen. Die Ergebnisse dieser Expertenberatungen werden gegebenenfalls in den Bericht gemäß Punkt 2.1 aufgenommen.