ISSN 1725-2598

Publicatieblad van de Europese Unie

L 210

Uitgave in de Nederlandse taal

Wetgeving

51e jaargang

6 augustus 2008

Inhoud

Prijs: 18 EUR

NL

Besluiten waarvan de titels mager zijn gedrukt, zijn besluiten van dagelijks beheer die in het kader van het landbouwbeleid zijn genomen en die in het algemeen een beperkte geldigheidsduur hebben.

Besluiten waarvan de titels vet zijn gedrukt en die worden voorafgegaan door een sterretje, zijn alle andere besluiten.

III

(Besluiten op grond van het EU-Verdrag)

BESLUITEN OP GROND VAN TITEL VI VAN HET EU-VERDRAG

BESLUIT 2008/615/JBZ VAN DE RAAD

van 23 juni 2008

inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit

DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag betreffende de Europese Unie, en met name op artikel 30, lid 1, onder a) en b), artikel 31, lid 1, onder a), artikel 32 en artikel 34, lid 2, onder c),

Gelet op het initiatief van het Koninkrijk België, de Republiek Bulgarije, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Franse Republiek, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden, de Republiek Oostenrijk, de Republiek Slovenië, de Slowaakse Republiek, de Italiaanse Republiek, de Republiek Finland, de Portugese Republiek, Roemenië en het Koninkrijk Zweden,

Gezien het advies van het Europees Parlement [1],

Overwegende hetgeen volgt:

(1) Naar aanleiding van de inwerkingtreding van het Verdrag tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Franse Republiek, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie (Verdrag van Prüm) wordt dit initiatief, in overleg met de Commissie, overeenkomstig de bepalingen van het Verdrag betreffende de Europese Unie, ingediend teneinde de inhoud van de bepalingen van het Verdrag van Prüm in het rechtskader van de Europese Unie te integreren.

(2) In de conclusies van de Europese Raad van Tampere in oktober 1999 wordt bevestigd dat met het oog op het opsporen en onderzoeken van strafbare feiten betere informatie-uitwisseling tussen de bevoegde instanties van de lidstaten nodig is.

(3) In het Haags programma betreffende de versterking van vrijheid, veiligheid en recht in de Europese Unie van november 2004, heeft de Europese Raad zijn overtuiging tot uitdrukking gebracht dat daartoe een innoverende benadering van de grensoverschrijdende uitwisseling van rechtshandhavingsinformatie nodig is.

(4) De Europese Raad heeft derhalve verklaard dat dergelijke informatie moet worden uitgewisseld volgens het beschikbaarheidsbeginsel. Dit betekent dat een rechtshandhavingsfunctionaris in een lidstaat van de Unie informatie die hij voor de uitoefening van zijn taak nodig heeft bij een andere lidstaat kan verkrijgen en dat de rechtshandhavingsinstanties in een lidstaat die over deze informatie beschikt, deze voor het aangegeven doel beschikbaar stellen, rekening houdend met de eisen van de lopende onderzoeken in die lidstaat.

(5) De Europese Raad stelde 1 januari 2008 vast als uiterste datum voor de verwezenlijking van deze doelstelling van het Haags programma.

(6) Kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsinstanties van de lidstaten van de Europese Unie [2] stelt reeds regels vast volgens welke de rechtshandhavingsinstanties van de lidstaten snel en doeltreffend bestaande informatie en inlichtingen kunnen uitwisselen teneinde een strafrechtelijk onderzoek uit te voeren of politie-inlichtingen te verzamelen.

(7) In het Haags programma betreffende de versterking van vrijheid, veiligheid en recht wordt echter ook verklaard dat ten volle gebruik moet worden gemaakt van nieuwe technologieën en dat ook wederzijdse toegang tot nationale databanken moet worden gefaciliteerd, terwijl het daarnaast bepaalt dat nieuwe gecentraliseerde Europese gegevensbestanden uitsluitend kunnen worden opgezet op basis van studies die de toegevoegde waarde ervan hebben aangetoond.

[1] Advies van 10 juni 2007 (nog niet in het Publicatieblad bekendgemaakt).

[2] PB L 386 van 29.12.2006, blz. 89.

(8) Met het oog op effectieve internationale samenwerking is het van fundamenteel belang dat nauwkeurige informatie snel en efficiënt kan worden uitgewisseld. Doel is procedures te introduceren ter bevordering van middelen voor snelle, efficiënte en goedkope gegevensuitwisseling. Met het oog op het gezamenlijk gebruik van gegevens moet met betrekking tot die procedures een verantwoordingsplicht gelden, en moeten de procedures de nodige waarborgen bieden wat betreft de juistheid en de beveiliging van de gegevens bij transmissie en opslag, en dienen er procedures te zijn voor de registratie van uitgewisselde gegevens en beperkingen op het gebruik van die gegevens.

(9) Aan die eisen is voldaan door middel van het Verdrag van Prüm, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie. Opdat aan de essentiële vereisten van het Haags programma voor alle lidstaten kan worden voldaan binnen het daarin vastgestelde tijdschema, moet de inhoud van de fundamentele onderdelen van het Verdrag van Prüm voor alle lidstaten van toepassing worden.

(10) Dit besluit bevat derhalve bepalingen die op de voornaamste bepalingen van het Verdrag van Prüm zijn gebaseerd en zijn bedoeld om de informatie-uitwisseling te bevorderen, en houdt in dat de lidstaten elkaar toegang verlenen tot hun geautomatiseerde DNA-analysebestanden, geautomatiseerde dactyloscopische identificatiesystemen en voertuigregisters. In het geval van nationale DNA-analysebestanden en geautomatiseerde dactyloscopische identificatiesystemen moet een hit/no hit-systeem de verzoekende lidstaat, in een tweede fase, in staat stellen specifieke met een dossier verband houdende persoonsgegevens op te vragen in de lidstaat die het dossier beheert en, waar nodig, via rechtshulpprocedures, waaronder die welke ingevolge Kaderbesluit 2006/960/JBZ zijn aangenomen, om nadere informatie te verzoeken.

(11) Dit zal de bestaande procedures aanzienlijk bespoedigen doordat de lidstaten zo kunnen nagaan of een andere lidstaat over de door hen benodigde informatie beschikt, en om welke lidstaat het gaat.

(12) Grensoverschrijdende gegevensvergelijking kan misdaadbestrijding een nieuwe dimensie geven. De informatie die door het vergelijken van gegevens wordt verkregen, moet voor de lidstaten de deur openen naar nieuwe onderzoeksmethoden en derhalve een cruciale rol spelen in het ondersteunen van de rechtshandhavings- en justitiële autoriteiten van de lidstaten.

(13) De regels zijn gebaseerd op het in een netwerk onderbrengen van de nationale databanken.

(14) Onder bepaalde voorwaarden moeten de lidstaten al dan niet persoonsgebonden gegevens kunnen verstrekken, zodat de uitwisseling van gegevens over grootschalige evenementen met een grensoverschrijdende dimensie wordt verbeterd met het oog op de voorkoming van strafbare feiten en de handhaving van de openbare orde en veiligheid.

(15) Bij de uitvoering van artikel 12 kunnen de lidstaten besluiten voorrang te geven aan de bestrijding van zware criminaliteit, gezien de beperkte technische capaciteit die beschikbaar is voor het doorzenden van gegevens.

(16) Niet alleen de verbeterde informatie-uitwisseling, maar ook andere vormen van nauwere samenwerking tussen politieautoriteiten moet worden gereguleerd, met name door middel van gezamenlijke veiligheidsoperaties (bv. gezamenlijke patrouilles).

(17) Nauwere politiële en justitiële samenwerking in strafzaken moet gepaard gaan met de eerbiediging van de grondrechten, met name het recht op eerbiediging van het privéleven en op de bescherming van persoonsgegevens, dat moet worden gewaarborgd door specifieke regelingen inzake gegevensbescherming, die moeten zijn toegesneden op de specifieke aard van verschillende vormen van gegevensuitwisseling. Dergelijke specifieke bepalingen inzake gegevensbescherming moeten met name rekening houden met het specifieke karakter van de grensoverschrijdende online toegang tot databanken. Aangezien bij online toegang de lidstaat die het dossier beheert geen voorafgaande controle kan uitvoeren, moet er een systeem worden opgezet dat ervoor zorgt dat controle achteraf plaatsvindt.

(18) Het hit/no hit-systeem biedt een structuur voor de vergelijking van anonieme profielen, waarbij aanvullende persoonsgegevens pas na een hit worden uitgewisseld, en het nationale recht, met inbegrip van de rechtshulpvoorschriften, bepalend is voor de verstrekking en de ontvangst van die gegevens. Deze opzet waarborgt een adequaat systeem voor gegevensbescherming, met dien verstande dat de verstrekking van persoonsgegevens aan een andere lidstaat een adequaat niveau van gegevensbescherming door de ontvangende lidstaten vereist.

(19) Gezien de ruime uitwisseling van informatie en gegevens ten gevolge van een nauwere politiële en justitiële samenwerking, wordt met dit besluit beoogd een passend niveau van gegevensbescherming te waarborgen. Er wordt rekening gehouden met het beschermingsniveau dat voor de verwerking van persoonsgegevens is vastgesteld in het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, het daarbij behorende Aanvullend Protocol van 8 november 2001 en de beginselen van Aanbeveling R (87) 15 van de Raad van Europa tot regeling van het gebruik van persoonsgegevens op politieel gebied.

(20) Tot de in dit besluit opgenomen bepalingen inzake gegevensbescherming behoren ook de beginselen inzake gegevensbescherming die noodzakelijk waren bij ontstentenis van een kaderbesluit inzake gegevensbescherming in de derde pijler. Dit Kaderbesluit zou moeten worden toegepast op het volledige gebied van de politiële en justitiële samenwerking in strafzaken, mits het niveau van gegevensbescherming waarin het voorziet, niet lager is dan dat van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens en het daarbij behorende Aanvullend Protocol van 8 november 2001, en daarbij rekening wordt gehouden met Aanbeveling R (87) 15 van het Comité van ministers van de Raad van Europa van 17 september 1987 tot regeling van het gebruik van persoonsgegevens op politieel gebied ook wanneer de gegevens niet geautomatiseerd worden verwerkt.

(21) Aangezien de doelstellingen van dit besluit, met name de verbetering van de informatie-uitwisseling in de Europese Unie, wegens het grensoverschrijdend karakter van misdaadbestrijding en veiligheidskwesties, niet afdoende door de lidstaten afzonderlijk kunnen worden verwezenlijkt zodat de lidstaten verplicht zijn hiervoor op elkaar een beroep te doen, kunnen zij beter op Europees niveau gerealiseerd worden. De Raad kan bijgevolg maatregelen aannemen volgens het subsidiariteitsbeginsel op grond van artikel 5 van het EG-Verdrag, waarnaar in artikel 2 van het EU-Verdrag wordt verwezen. Overeenkomstig het in artikel 5 van het EG-Verdrag neergelegde evenredigheidsbeginsel gaat dit besluit niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(22) Dit besluit is in overeenstemming met de grondrechten en beginselen die met name in het Handvest van de grondrechten van de Europese Unie neergelegd zijn,

BESLUIT:

HOOFDSTUK 1

ALGEMENE ASPECTEN

Artikel 1

Doel en werkingssfeer

De lidstaten beogen met dit besluit de grensoverschrijdende samenwerking, op gebieden die onder titel VI van het Verdrag vallen, te intensiveren, met name de uitwisseling van informatie tussen instanties die met de voorkoming en opsporing van strafbare feiten belast zijn. Daartoe bevat dit besluit regels op de volgende gebieden:

a) bepalingen over de voorwaarden en de procedure voor de geautomatiseerde overdracht van DNA-profielen, dactyloscopische gegevens en bepaalde gegevens uit de nationale kentekenregisters (Hoofdstuk 2);

b) bepalingen over de voorwaarden voor gegevensverstrekking in het kader van grootschalige evenementen met een grensoverschrijdende dimensie (Hoofdstuk 3);

c) bepalingen over de voorwaarden voor de verstrekking van informatie ter voorkoming van terroristische misdrijven (Hoofdstuk 4);

d) bepalingen over de voorwaarden en de procedure voor de intensivering van de grensoverschrijdende politiële samenwerking via diverse maatregelen (Hoofdstuk 5).

HOOFDSTUK 2

ONLINE TOEGANG EN VERVOLGVERZOEKEN

DEEL 1

DNA-profielen

Artikel 2

Aanleggen van nationale DNA-analysebestanden

1. De lidstaten leggen ter opsporing van strafbare feiten nationale DNA-analysebestanden aan en beheren deze. De verwerking van de op grond van dit besluit in deze bestanden opgeslagen gegevens geschiedt behoudens de overige bepalingen van dit besluit, met inachtneming van het voor de verwerking geldende nationale recht.

2. Ter uitvoering van dit besluit waarborgen de lidstaten dat linkgegevens uit het nationale DNA-analysebestand, als bedoeld in lid 1, eerste zin, aanwezig zijn. Linkgegevens omvatten uitsluitend de op basis van het niet-gecodeerde gedeelte van het DNA vastgestelde DNA-profielen en een kenmerk. De linkgegevens mogen geen gegevens bevatten waarmee de betrokkene rechtstreeks kan worden geïdentificeerd. Linkgegevens die niet op een persoon terug te voeren zijn (ongeïdentificeerde DNA-profielen), dienen als zodanig herkenbaar te zijn.

3. Elke lidstaat deelt overeenkomstig artikel 36 het secretariaat-generaal van de Raad de nationale DNA-analysebestanden, waarop de artikelen 2 tot en met 6 van toepassing zijn, alsmede de voorwaarden voor de geautomatiseerde bevraging, bedoeld in artikel 3, lid 1, mee.

Artikel 3

Geautomatiseerde bevraging van DNA-profielen

1. Ter opsporing van strafbare feiten verlenen de lidstaten aan de nationale contactpunten van de andere lidstaten, bedoeld in artikel 6, toegang tot de linkgegevens van hun DNA-analysebestanden, met het recht deze geautomatiseerd te bevragen door middel van een vergelijking van de DNA-profielen. De bevoegdheid tot bevraging mag uitsluitend in individuele gevallen en met inachtneming van het nationale recht van de verzoekende lidstaat worden uitgeoefend.

2. Indien bij een geautomatiseerde bevraging wordt vastgesteld dat een verstrekt DNA-profiel overeenkomt met een in het bestand van de ontvangende lidstaat opgeslagen DNA-profiel, dan ontvangt het nationale contactpunt van de verzoekende lidstaat langs geautomatiseerde weg de informatie over de linkgegevens waarmee een overeenkomst is vastgesteld. Indien geen overeenkomst kan worden vastgesteld, wordt zulks geautomatiseerd meegedeeld.

Artikel 4

Geautomatiseerde vergelijking van DNA-profielen

1. Ter opsporing van strafbare feiten vergelijken de lidstaten met wederzijds goedvinden via hun nationale contactpunten hun ongeïdentificeerde DNA-profielen met alle DNA-profielen uit linkgegevens van de andere nationale DNA-analysebestanden. Verstrekking en vergelijking geschieden geautomatiseerd. Verstrekking ter vergelijking van ongeïdentificeerde DNA-profielen geschiedt uitsluitend in die gevallen waarin het nationale recht van de verzoekende lidstaat hierin voorziet.

2. Indien een lidstaat bij de vergelijking, bedoeld in het eerste lid, vaststelt dat verstrekte DNA-profielen met enig profiel in zijn DNA-analysebestand overeenkomen, verstrekt hij onverwijld aan het nationale contactpunt van de andere lidstaat de linkgegevens waarmee een overeenkomst is vastgesteld.

Artikel 5

Verstrekking van nadere persoonsgegevens en overige informatie

Indien in het kader van de procedure, bedoeld in de artikelen 3 en 4, wordt vastgesteld dat DNA-profielen overeenkomen, is het nationale recht, met inbegrip van de rechtshulpvoorschriften, van de aangezochte lidstaat bepalend voor de verstrekking van nadere, met betrekking tot de linkgegevens beschikbare persoonsgegevens en overige informatie.

Artikel 6

Nationaal contactpunt en uitvoeringsmaatregelen

1. Ter uitvoering van de gegevensverstrekking, bedoeld in de artikelen 3 en 4, wijst elke lidstaat een nationaal contactpunt aan. De bevoegdheden van het nationale contactpunt worden bepaald door het hierop van toepassing zijnde nationale recht.

2. De bijzonderheden met betrekking tot de technische regelingen voor de in de artikelen 3 en 4 beschreven procedures worden door middel van de uitvoeringsmaatregelen als bedoeld in artikel 33 geregeld.

Artikel 7

Afname van celmateriaal en verstrekking van DNA-profielen

Indien in het kader van een lopend opsporingsonderzoek of strafrechtelijke procedure geen DNA-profiel beschikbaar is van een bepaalde persoon die zich op het grondgebied van een aangezochte lidstaat bevindt, verleent de aangezochte lidstaat rechtshulp door het afnemen en onderzoeken van celmateriaal van deze persoon evenals door verstrekking van het verkregen DNA-profiel, indien:

a) de verzoekende lidstaat meedeelt voor welk doel zulks vereist is;

b) de verzoekende lidstaat een naar het recht van die staat vereist onderzoeksbevel of verklaring van de bevoegde autoriteit overlegt, waaruit blijkt dat aan de voorwaarden voor het afnemen en onderzoeken van celmateriaal zou zijn voldaan indien de desbetreffende persoon zich op het grondgebied van de verzoekende lidstaat zou bevinden, en

c) naar het recht van de aangezochte lidstaat aan de voorwaarden voor het afnemen en onderzoeken van celmateriaal alsmede aan de voorwaarden voor de verstrekking van het verkregen DNA-profiel, is voldaan.

DEEL 2

Dactyloscopische gegevens

Artikel 8

Dactyloscopische gegevens

Ter uitvoering van dit besluit zien de lidstaten erop toe dat linkgegevens uit het bestand van de ter voorkoming en opsporing van strafbare feiten opgezette nationale geautomatiseerde dactyloscopische identificatiesystemen beschikbaar zijn. Linkgegevens omvatten uitsluitend dactyloscopische gegevens en een kenmerk. De linkgegevens mogen geen gegevens bevatten waarmee de betrokkene rechtstreeks kan worden geïdentificeerd. Linkgegevens die niet op een persoon terug te voeren zijn (ongeïdentificeerde dactyloscopische gegevens) dienen als zodanig herkenbaar te zijn.

Artikel 9

Geautomatiseerde bevraging van dactyloscopische gegevens

1. Ter voorkoming en opsporing van strafbare feiten verlenen de lidstaten aan de nationale contactpunten van de andere lidstaten, bedoeld in artikel 11, toegang tot de linkgegevens van de geautomatiseerde dactyloscopische identificatiesystemen die zij daartoe hebben opgezet, zulks met het recht deze geautomatiseerd te bevragen door middel van een vergelijking van de dactyloscopische gegevens. De bevoegdheid tot bevraging mag uitsluitend in individuele gevallen en met inachtneming van het nationale recht van de verzoekende lidstaat worden uitgeoefend.

2. De definitieve koppeling van een dactyloscopisch gegeven aan een linkgegeven van de met het bestandsbeheer belaste lidstaat geschiedt door het nationale contactpunt van de verzoekende lidstaat aan de hand van de geautomatiseerd verstrekte linkgegevens, die voor de eenduidige koppeling noodzakelijk zijn.

Artikel 10

Verstrekking van nadere persoonsgegevens en overige informatie

Indien in het kader van de procedure, als bedoeld in artikel 9, wordt vastgesteld dat dactyloscopische gegevens overeenkomen, is het nationale recht, met inbegrip van de rechtshulpvoorschriften, van de aangezochte lidstaat bepalend voor de verstrekking van nadere, met betrekking tot de linkgegevens beschikbare persoonsgegevens en overige informatie.

Artikel 11

Nationaal contactpunt en uitvoeringsmaatregelen

1. Ter uitvoering van de gegevensverstrekking, als bedoeld in artikel 9, wijst elke lidstaat een nationaal contactpunt aan. De bevoegdheden van het nationale contactpunt worden bepaald door het hierop van toepassing zijnde nationale recht.

2. De bijzonderheden met betrekking tot de technische regelingen voor de in artikel 9 beschreven procedure worden door middel van de uitvoeringsmaatregelen als bedoeld in artikel 33 geregeld.

DEEL 3

Gegevens uit de kentekenregisters

Artikel 12

Geautomatiseerde bevraging van gegevens uit de kentekenregisters

1. Ter voorkoming en opsporing van strafbare feiten alsmede ter afhandeling van overtredingen die in de verzoekende lidstaat tot de bevoegdheid van de rechtbanken of het openbaar ministerie behoren, en ter handhaving van de openbare orde en veiligheid, verlenen de lidstaten aan de nationale contactpunten van de andere lidstaten, bedoeld in lid 2, toegang tot de volgende gegevens uit de nationale kentekenregisters, zulks met het recht deze in individuele gevallen geautomatiseerd te bevragen:

a) gegevens met betrekking tot de eigenaars of houders, en

b) gegevens met betrekking tot voertuigen.

De bevraging mag uitsluitend met gebruikmaking van een volledig chassisnummer of een volledig kenteken worden gedaan. De bevoegdheid tot bevraging mag uitsluitend met inachtneming van het nationale recht van de verzoekende lidstaat worden uitgeoefend.

2. Ter uitvoering van de gegevensuitwisseling, bedoeld in lid 1, wijst elke lidstaat een nationaal contactpunt voor inkomende verzoeken aan. De bevoegdheden van het nationale contactpunt worden bepaald door het hierop van toepassing zijnde nationale recht. De bijzonderheden met betrekking tot de technische regelingen voor de procedure worden door middel van de uitvoeringsmaatregelen als bedoeld in artikel 33 geregeld.

HOOFDSTUK 3

GROOTSCHALIGE EVENEMENTEN

Artikel 13

Verstrekking van niet-persoonsgebonden gegevens

Ter voorkoming van strafbare feiten en ter handhaving van de openbare orde en veiligheid in samenhang met grootschalige evenementen met een grensoverschrijdende dimensie, in het bijzonder sportmanifestaties of bijeenkomsten van de Europese Raad, verstrekken de lidstaten elkaar zowel op verzoek als op eigen initiatief, met inachtneming van het nationale recht van de verstrekkende lidstaat, niet-persoonsgebonden gegevens die hiertoe noodzakelijk kunnen zijn.

Artikel 14

Verstrekking van persoonsgebonden gegevens

1. Ter voorkoming van strafbare feiten en ter handhaving van de openbare orde en veiligheid in samenhang met grootschalige evenementen met een grensoverschrijdende dimensie, in het bijzonder sportmanifestaties of bijeenkomsten van de Europese Raad, verstrekken de lidstaten elkaar zowel op verzoek als op eigen initiatief persoonsgegevens, indien definitieve veroordelingen of andere feiten het vermoeden rechtvaardigen dat de desbetreffende personen tijdens de evenementen strafbare feiten zullen plegen of dat zij een gevaar voor de openbare orde en veiligheid vormen, voor zover de verstrekking van deze gegevens overeenkomstig het nationale recht van de verstrekkende lidstaat is toegestaan.

2. De persoonsgegevens mogen uitsluitend worden verwerkt voor de in lid 1 omschreven doeleinden en in het kader van de nauwkeurig omschreven evenementen waarvoor deze werden meegedeeld. De verstrekte gegevens dienen onverwijld te worden gewist zodra de doeleinden, bedoeld in lid 1, zijn verwezenlijkt of niet meer verwezenlijkt kunnen worden. De verstrekte gegevens dienen in elk geval uiterlijk na een jaar te worden gewist.

Artikel 15

Nationaal contactpunt

Ter uitvoering van de gegevensverstrekking, bedoeld in de artikelen 13 en 14, wijst elke lidstaat een nationaal contactpunt aan. De bevoegdheden van het nationale contactpunt worden bepaald door het hierop van toepassing zijnde nationale recht.

HOOFDSTUK 4

MAATREGELEN TER VOORKOMING VAN TERRORISTISCHE MISDRIJVEN

Artikel 16

Verstrekking van informatie ter voorkoming van terroristische misdrijven

1. Ter voorkoming van terroristische misdrijven kunnen lidstaten aan de nationale contactpunten van andere lidstaten, bedoeld in lid 3, met inachtneming van het nationale recht, in individuele gevallen, ook zonder verzoek de in lid 2 genoemde persoonsgegevens en informatie verstrekken, voor zover zulks noodzakelijk is omdat bepaalde feiten het vermoeden rechtvaardigen dat de betrokkenen strafbare feiten zullen plegen als bedoeld in de artikelen 1 tot en met 3 van Kaderbesluit 2002/475/JBZ van de Raad van 13 juni 2002 inzake terrorismebestrijding ([1]).

([1]) PB L 164 van 22.6.2002, blz. 3.

2. De te verstrekken gegevens en informatie omvatten namen, voornamen, geboortedatum en geboorteplaats alsmede de beschrijving van de omstandigheden die aanleiding geven tot het vermoeden, bedoeld in lid 1.

3. Elke lidstaat wijst een nationaal contactpunt aan dat is belast met de gegevensuitwisseling met de nationale contactpunten van de andere lidstaat. De bevoegdheden van het nationale contactpunt worden bepaald door het hierop van toepassing zijnde nationale recht.

4. De verstrekkende lidstaat kan, met inachtneming van het nationale recht, voorwaarden verbinden aan het gebruik van deze gegevens en informatie door de ontvangende lidstaat. De ontvangende lidstaat is aan deze voorwaarden gebonden.

HOOFDSTUK 5

ANDERE SAMENWERKINGSVORMEN

Artikel 17

Gezamenlijk optreden

1. Ter intensivering van de politiële samenwerking kunnen de door de lidstaten aangewezen bevoegde autoriteiten gezamenlijke patrouilles en andere vormen van gezamenlijk optreden ter handhaving van de openbare orde en veiligheid en ter voorkoming van strafbare feiten instellen, waarbij de door de lidstaten aangewezen ambtenaren of ander overheidspersoneel („ambtenaren"), van andere lidstaten aan het optreden op het grondgebied van een lidstaat meewerken.

2. Elke lidstaat kan als gastlidstaat, met inachtneming van zijn nationale recht, ambtenaren van andere lidstaten met toestemming van de zendlidstaat in het kader van een gezamenlijk optreden uitvoerende bevoegdheden toekennen of, voor zover zulks naar het recht van de gastlidstaat is toegestaan, ambtenaren van andere lidstaten toestaan hun uitvoerende bevoegdheden overeenkomstig het recht van de zendlidstaat uit te oefenen. Deze uitvoerende bevoegdheden mogen hierbij uitsluitend onder leiding en, in beginsel, in aanwezigheid van ambtenaren van de gastlidstaat worden uitgeoefend. De ambtenaren van de andere lidstaten zijn hierbij aan het nationale recht van de gastlidstaat gebonden. Hun handelen valt onder de verantwoordelijkheid van de gastlidstaat.

3. Bij een gezamenlijk optreden betrokken ambtenaren van andere lidstaten zijn onderworpen aan de aanwijzingen van de bevoegde autoriteit van de gastlidstaat.

4. De lidstaten dienen een verklaring in als bedoeld in artikel 37 waarin zij de praktische aspecten van de samenwerking vaststellen.

Artikel 18

Bijstand in verband met massabijeenkomsten, rampen en zware ongevallen

De bevoegde autoriteiten van de lidstaten verlenen elkaar met inachtneming van het nationale recht wederzijds bijstand bij massabijeenkomsten en vergelijkbaar grootschalige gebeurtenissen, rampen en zware ongevallen, waarbij zij trachten strafbare feiten te voorkomen en de openbare orde en veiligheid te handhaven door:

a) elkaar zo vroeg mogelijk over dergelijke situaties met grensoverschrijdende gevolgen te informeren en relevante informatie uit te wisselen;

b) in situaties met grensoverschrijdende gevolgen de op hun grondgebied noodzakelijke politiemaatregelen te treffen en te coördineren;

c) op verzoek van de lidstaat op wiens grondgebied de situatie zich voordoet, voor zover mogelijk, ambtenaren, specialisten en adviseurs uit te zenden en uitrusting ter beschikking te stellen.

Artikel 19

Gebruik van bewapening, munitie en uitrusting

1. Ambtenaren van een lidstaat die zich in het kader van een gezamenlijk optreden ingevolge artikel 17 of 18 op het grondgebied van een andere lidstaat bevinden, kunnen ter plaatse hun nationale dienstkleding dragen. Zij kunnen daar hun naar het nationale recht van de zendlidstaat toegestane bewapening, munitie en uitrusting meedragen. Elke gastlidstaat kan het meevoeren van bepaalde bewapening, munitie en uitrusting door ambtenaren van de zendlidstaat verbieden.

2. De lidstaten brengen verklaringen uit als bedoeld in artikel 36 waarin bewapening, munitie en uitrusting worden opgesomd die uitsluitend mogen worden gebruikt bij wettige zelfverdediging of ter verdediging van anderen. De met de feitelijke leiding belaste ambtenaar van de gastlidstaat kan in individuele gevallen met inachtneming van het nationale recht toestemming verlenen voor gebruik van bewapening, munitie en uitrusting dat verder reikt dan het bepaalde in de eerste volzin. Het gebruik van de bewapening, munitie en uitrusting wordt bepaald door het recht van de gastlidstaat. De bevoegde autoriteiten informeren elkaar over de toegestane bewapening, munitie en uitrusting alsmede over de voorwaarden voor het gebruik ervan.

3. Indien ambtenaren van de ene lidstaat bij maatregelen op grond van dit besluit op het grondgebied van een andere lidstaat voertuigen inzetten, zijn zij aan dezelfde verkeersregels, met inbegrip van de voorrangsrechten en speciale voorrechten, onderworpen als de ambtenaren van de gastlidstaat.

4. De lidstaten leggen verklaringen over als bedoeld in artikel 36 waarin zij de praktische aspecten van het gebruik van bewapening, munitie en uitrusting vaststellen.

Artikel 20

Bescherming en bijstand

De lidstaten zijn jegens de grensoverschrijdende ambtenaren van de andere lidstaten tijdens de dienstuitoefening tot dezelfde bescherming en bijstand verplicht als jegens de eigen ambtenaren.

Artikel 21

Algemene civielrechtelijke aansprakelijkheidsregeling

1. Wanneer ambtenaren van een lidstaat in een andere lidstaat optreden overeenkomstig artikel 17, is de eerstgenoemde lidstaat overeenkomstig het recht van de lidstaat op het grondgebied waarvan zij optreden aansprakelijk voor de schade die zij aldaar tijdens hun optreden veroorzaken.

2. De lidstaat op het grondgebied waarvan de in lid 1 bedoelde schade wordt veroorzaakt, vergoedt deze schade op dezelfde wijze als schade die door zijn eigen ambtenaren wordt toegebracht.

3. In het in lid 1 bedoelde geval betaalt de lidstaat waarvan de ambtenaren op het grondgebied van een andere lidstaat aan een persoon schade hebben veroorzaakt, aan die andere lidstaat het volledige bedrag terug dat deze aan de slachtoffers of hun rechthebbenden heeft uitgekeerd.

4. Wanneer ambtenaren van een lidstaat in een andere lidstaat optreden overeenkomstig artikel 18, is de laatstgenoemde lidstaat overeenkomstig zijn nationale recht aansprakelijk voor de schade die zij aldaar tijdens hun optreden veroorzaken.

5. Wanneer de in lid 4 bedoelde schade het gevolg is van grove nalatigheid of opzettelijk wangedrag, kan de gastlidstaat de zendlidstaat benaderen om van deze laatste terugbetaling te verkrijgen van de bedragen die deze aan de slachtoffers of hun rechthebbenden heeft uitgekeerd.

6. Onder voorbehoud van de uitoefening van zijn rechten tegenover derden en met uitzondering van het bepaalde in lid 3 ziet elke lidstaat, in het geval bedoeld in lid 1, ervan af het bedrag van de door hem geleden schade op een andere lidstaat te verhalen.

Artikel 22

Strafrechtelijke aansprakelijkheid

De ambtenaren die uit hoofde van dit besluit op het grondgebied van een gastlidstaat optreden, worden gelijkgesteld met de ambtenaren van die andere lidstaat wat betreft strafbare feiten die door of tegen hen worden gepleegd, tenzij in een andere voor de betrokken lidstaten bindende overeenkomst anders is overeengekomen.

Artikel 23

Dienstbetrekking

Op ambtenaren die uit hoofde van dit besluit op het grondgebied van een andere lidstaat optreden, blijven in arbeidsrechtelijk, en in het bijzonder in tuchtrechtelijk opzicht de in hun lidstaat geldende voorschriften van toepassing.

HOOFDSTUK 6

ALGEMENE BEPALINGEN BETREFFENDE GEGEVENSBESCHERMING

Artikel 24

Definities en toepassingsgebied

1. In dit besluit wordt verstaan onder:

a) „verwerking van persoonsgegevens": elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken of wijzigen, selecteren, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Als verwerking in de zin van dit besluit geldt ook de mededeling of er al dan niet een hit gevonden is;

b) „geautomatiseerde bevraging": de directe toegang tot een geautomatiseerd bestand van een andere instantie, en wel op zodanige wijze dat de bevraging volledig geautomatiseerd wordt beantwoord;

c) „kenmerken": het markeren van opgeslagen persoonsgegevens, zonder dat daarmee het doel wordt nagestreefd om hun toekomstige verwerking te beperken;

d) „afscherming": het markeren van opgeslagen persoonsgegevens met het doel hun toekomstige verwerking te beperken.

2. Voor gegevens die uit hoofde van dit besluit worden of zijn verstrekt gelden de volgende bepalingen, tenzij in de voorafgaande hoofdstukken anderszins is bepaald.

Artikel 25

Niveau van gegevensbescherming

1. Elke lidstaat waarborgt met betrekking tot de verwerking van persoonsgegevens die uit hoofde van dit besluit worden of zijn verstrekt, in het nationale recht een gegevensbeschermingsniveau dat ten minste overeenstemt met datgene dat voortvloeit uit het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens en het daarbij behorende Aanvullend Protocol van 8 november 2001, en houdt daarbij rekening met Aanbeveling R (87) 15 van het Comité van ministers van de Raad van Europa aan de lidstaten over het gebruik van persoonsgegevens op politieel gebied van 17 september 1987, ook wanneer de gegevens niet geautomatiseerd worden verwerkt.

2. Met de in dit besluit voorziene verstrekking van persoonsgegevens mag pas worden begonnen nadat op het grondgebied van de bij de verstrekking betrokken lidstaten de bepalingen van dit hoofdstuk in het nationale recht zijn verwerkt. De Raad besluit met eenparigheid van stemmen of aan deze voorwaarde is voldaan.

3. Lid 2 is niet van toepassing op de lidstaten waar met de in dit besluit voorziene verstrekking van persoonsgegevens reeds is begonnen op grond van het Verdrag van 27 mei 2005 tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Franse Republiek, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie (Verdrag van Prüm).

Artikel 26

Doelbinding

1. De ontvangende lidstaat mag de persoonsgegevens uitsluitend verwerken voor de doeleinden waarvoor deze op grond van dit besluit zijn verstrekt; verwerking voor andere doeleinden is alleen toegestaan na voorafgaande toestemming van de lidstaat die het dossier beheert en mag uitsluitend beheerd worden door het nationale recht van de ontvangende lidstaat. De toestemming mag worden verleend voor zover op grond van het nationale recht van de lidstaat die het bestand beheert deze verwerking voor zulke andere doeleinden is toegestaan.

2. De verwerking van de op grond van de artikelen 3, 4 en 9 verstrekte gegevens door de bevragende of vergelijkende lidstaat is uitsluitend toegestaan met het oog op:

a) de vaststelling of de vergeleken DNA-profielen of dactyloscopische gegevens overeenstemmen;

b) de voorbereiding en indiening van een politieel of justitieel verzoek om rechtshulp conform nationaal recht in geval van overeenstemming van deze gegevens;

c) de protocollering als bedoeld in artikel 30.

De lidstaat die het dossier beheert mag de hem op grond van de artikelen 3, 4 en 9 verstrekte gegevens uitsluitend verwerken voor zover dit voor het uitvoeren van de vergelijking, het geautomatiseerde beantwoorden van de bevraging of het protocolleren als bedoeld in artikel 30 noodzakelijk is. Na afloop van de gegevensvergelijking of na de geautomatiseerde beantwoording van de bevraging worden de verstrekte gegevens onverwijld gewist, tenzij verdere verwerking noodzakelijk is ten behoeve van de doelen genoemd in de eerste alinea, onder b) en c).

3. Uit hoofde van artikel 12 verstrekte gegevens mogen door de lidstaat die het dossier beheert uitsluitend worden gebruikt voor zover dit voor het geautomatiseerd beantwoorden van de bevraging of het protocolleren als bedoeld in artikel 30 noodzakelijk is. Na de geautomatiseerde beantwoording van de bevraging worden de verstrekte gegevens onverwijld gewist, tenzij verdere verwerking noodzakelijk is voor het protocolleren op grond van artikel 30. De bevragende lidstaat mag de in het kader van de beantwoording verkregen gegevens uitsluitend gebruiken voor de procedure op grond waarvan de bevraging is geschied.

Artikel 27

Bevoegde autoriteiten

De verstrekte persoonsgegevens mogen uitsluitend door de autoriteiten, instanties en rechtbanken worden verwerkt die bevoegd zijn voor een taak in het kader van de in artikel 26 genoemde doeleinden. In het bijzonder vindt de doorzending van de verstrekte gegevens aan andere instanties alleen plaats na voorafgaande toestemming van de verstrekkende lidstaat en met inachtneming van het recht van de ontvangende lidstaat.

Artikel 28

Juistheid, actualiteit en opslagduur van de gegevens

1. De lidstaten staan borg voor de juistheid en de actualiteit van de persoonsgegevens. Als blijkt, ambtshalve of op basis van een mededeling van de betrokkene, dat onjuiste gegevens of gegevens die niet hadden mogen worden verstrekt, toch verstrekt zijn, dan wordt dit onverwijld aan de ontvangende lidstaat of lidstaten meegedeeld. De betrokken lidstaat is, c.q. de betrokken lidstaten zijn, verplicht de gegevens te corrigeren of te wissen. Voor het overige worden verstrekte persoonsgegevens gecorrigeerd als blijkt dat ze onjuist zijn. Als de ontvangende instantie reden heeft om aan te nemen dat de verstrekte gegevens onjuist zijn of gewist moeten worden, dan stelt zij de verstrekkende autoriteit daarvan onverwijld op de hoogte.

2. Gegevens waarvan de betrokkene de juistheid aanvecht en waarvan de juistheid of onjuistheid niet kan worden vastgesteld, moeten met inachtneming van het nationale recht van de lidstaten op verzoek van de betrokkene worden gemarkeerd. Indien er een markering is aangebracht mag deze met inachtneming van het nationale recht van de lidstaten alleen met toestemming van de betrokkene of op basis van een besluit van de bevoegde rechtbank of de voor de gegevensbescherming bevoegde onafhankelijke instantie worden opgeheven.

3. Verstrekte persoonsgegevens worden gewist als ze niet verstrekt of ontvangen hadden mogen worden. Rechtmatig verstrekte en ontvangen gegevens worden gewist:

a) als ze voor het doel waarvoor ze zijn verstrekt, niet of niet meer noodzakelijk zijn; als persoonsgegevens ongevraagd zijn verstrekt, moet de ontvangende instantie onverwijld controleren of ze noodzakelijk zijn voor het doel waarvoor ze zijn verstrekt;

b) na afloop van een in het nationale recht van de verstrekkende lidstaat voorziene maximale termijn voor het bewaren van de gegevens, als de verstrekkende instantie de ontvangende instantie bij de verstrekking op die maximale termijn heeft gewezen.

Als er reden bestaat om aan te nemen dat door het wissen de belangen van de betrokkene worden geschaad, worden de gegevens afgeschermd in plaats van gewist, overeenkomstig het nationale recht. Afgeschermde gegevens mogen alleen worden verstrekt of gebruikt voor het doel dat ertoe heeft geleid dat ze niet zijn gewist.

Artikel 29

Technische en organisatorische maatregelen ter bescherming en beveiliging van gegevens

1. De verstrekkende en de ontvangende instantie zijn verplicht om persoonsgegevens effectief te beschermen tegen toevallige of onbevoegde vernietiging, toevallig verlies, onbevoegde toegang, onbevoegde of toevallige verandering en onbevoegde bekendmaking.

2. De bijzonderheden van de technische vormgeving van de geautomatiseerde bevragingsprocedure worden geregeld in uitvoeringsmaatregelen zoals bedoeld in artikel 33, die waarborgen dat:

a) aan de huidige stand van de techniek aangepaste maatregelen ter waarborging van de bescherming en de beveiliging van gegevens worden getroffen, die in het bijzonder de vertrouwelijkheid en de integriteit van de gegevens waarborgen;

b) bij het gebruik van algemeen toegankelijke netwerken door de daarvoor bevoegde instanties erkende versleutelings- en autorisatieprocedures worden gebruikt, en

c) dat de toelaatbaarheid van de bevragingen in overeenstemming met artikel 30, leden 2, 4 en 5, kan worden gecontroleerd.

Artikel 30

Vastleggen en protocolleren; bijzondere voorschriften met betrekking tot de geautomatiseerde en niet-geautomatiseerde verstrekking

1. Elke lidstaat waarborgt dat iedere niet-geautomatiseerde verstrekking en iedere niet-geautomatiseerde ontvangst van persoonsgegevens door de instantie die het bestand beheert en de bevragende instantie ter controle van de toelaatbaarheid van de verstrekking wordt vastgelegd. De vastlegging omvat de volgende gegevens:

a) de aanleiding van de verstrekking;

b) de verstrekte gegevens;

c) de datum van de verstrekking, en

d) de aanduiding of de code van de bevragende instantie en de instantie die het bestand beheert.

2. Voor de geautomatiseerde bevraging van gegevens op grond van de artikelen 3, 9 en 12 of geautomatiseerde vergelijking uit hoofde van artikel 4 geldt het volgende:

a) Geautomatiseerde bevraging of vergelijking mag alleen geschieden door speciaal daartoe gemachtigde ambtenaren van de nationale contactpunten. Op verzoek wordt de lijst van ambtenaren die zijn gemachtigd tot geautomatiseerde bevraging of vergelijking aan de in lid 5 bedoelde toezichthoudende autoriteiten en aan de andere lidstaten ter beschikking gesteld.

b) Elke lidstaat waarborgt dat iedere verstrekking en iedere ontvangst van persoonsgegevens door de instantie die het dossier beheert en de bevragende instantie wordt geprotocolleerd, inclusief de kennisgeving ten aanzien van het al dan niet bestaan van een hit. De protocollering omvat de volgende informatie:

i) de verstrekte gegevens;

ii) de datum en het precieze tijdstip van de verstrekking, en

iii) de aanduiding of de code van de bevragende instantie en de instantie die het bestand beheert.

De bevragende instantie protocolleert bovendien de aanleiding van de bevraging of verstrekking alsmede het kenmerk van de ambtenaar die de bevraging heeft uitgevoerd en de ambtenaar die opdracht tot bevraging of verstrekking heeft gegeven.

3. De protocollerende instantie deelt op verzoek de geprotocolleerde gegevens onverwijld mee aan de voor de controle van de gegevensbescherming bevoegde autoriteiten van de desbetreffende lidstaat en dit uiterlijk binnen vier weken na ontvangst van het verzoek. Geprotocolleerde gegevens mogen uitsluitend worden gebruikt voor de volgende doeleinden:

a) de controle van de gegevensbescherming;

b) het waarborgen van de dataveiligheid.

4. De geprotocolleerde gegevens worden door passende voorzieningen tegen oneigenlijk gebruik en andere vormen van misbruik beschermd en twee jaar bewaard. Na afloop van de bewaringstermijn worden de geprotocolleerde gegevens onverwijld gewist.

5. De juridische controle van de verstrekking of de ontvangst van persoonsgegevens is in handen van de voor de gegevensbescherming bevoegde onafhankelijke instanties of, in voorkomend geval, de justitiële autoriteiten van de respectieve lidstaten. Met inachtneming van het nationale recht kan eenieder deze instanties verzoeken om de rechtmatigheid van de verwerking van gegevens met betrekking tot zijn persoon te controleren. Deze instanties alsmede de voor de protocollering bevoegde instanties voeren ook, los van dergelijke verzoeken, bij wijze van steekproef controles uit ten aanzien van de rechtmatigheid van de verstrekkingen, en wel aan de hand van de betrokken bestanden.

De resultaten van deze controleactiviteit worden ter controle door de voor de gegevensbescherming bevoegde onafhankelijke instanties gedurende 18 maanden bewaard. Na afloop van deze termijn worden ze onverwijld gewist. Elke voor de gegevensbescherming bevoegde instantie kan door de voor gegevensbescherming bevoegde onafhankelijke instantie van een andere lidstaat in overeenstemming met het nationale recht om de uitoefening van haar bevoegdheden worden verzocht. De voor de gegevensbescherming bevoegde onafhankelijke instanties van de lidstaten dragen zorg voor de ter vervulling van hun controletaken noodzakelijke wederzijdse samenwerking, in het bijzonder door het uitwisselen van relevante informatie.

Artikel 31

Recht van de betrokkene op informatie en schadevergoeding

1. Aan de betrokkene dient met inachtneming van het nationale recht, na overlegging van bewijs van zijn identiteit, op verzoek van de op grond van het nationale recht bevoegde instantie, zonder onredelijke kosten, in algemeen begrijpelijke vorm en zonder onaanvaardbare vertraging informatie te worden verstrekt over de met betrekking tot zijn persoon verwerkte gegevens alsmede over de herkomst daarvan, de ontvanger of ontvangercategorieën, het beoogde doel van de verwerking en, wanneer zulks op grond van het nationale recht vereist is, de rechtsgrond voor de verwerking. Bovendien heeft de betrokkene recht op correctie van onjuiste gegevens en op het wissen van onrechtmatig verwerkte gegevens. De lidstaten dragen er bovendien zorg voor dat de betrokkene in geval van inbreuk op zijn rechten met betrekking tot gegevensbescherming een klacht kan indienen bij een onafhankelijke rechtbank of een tribunaal in de zin van artikel 6, lid 1, van het Europese Verdrag voor de rechten van de mens of bij een onafhankelijke controle-instantie in de zin van artikel 28 van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 ([1]) betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en dat hij aanspraak op schadevergoeding kan maken of om een andere vorm van genoegdoening kan verzoeken. De nadere bijzonderheden met betrekking tot de procedure ter verwezenlijking van deze rechten en de redenen voor het beperken van het recht op toegang worden beheerst door de desbetreffende nationale wettelijke voorschriften van de lidstaat waarin de betrokkene zijn rechten doet gelden.

2. Als een instantie van een lidstaat persoonsgegevens heeft verstrekt uit hoofde van dit besluit, kan de ontvangende instantie van de andere lidstaat zich niet beroepen op de onjuistheid van de verstrekte gegevens om haar aansprakelijkheid jegens de benadeelde partij krachtens het nationale recht te ontlopen. Moet de ontvangende instantie schade vergoeden wegens het gebruik van onjuist doorgegeven gegevens, dan betaalt de verstrekkende instantie de ontvangende instantie het volledige bedrag aan schadevergoeding terug.

Artikel 32

Door de lidstaten gevraagde informatie

De ontvangende lidstaat informeert de verstrekkende lidstaat op verzoek over de verwerking van de verstrekte gegevens en het resultaat daarvan.

HOOFDSTUK 7

UITVOERINGS- EN SLOTBEPALINGEN

Artikel 33

Uitvoeringsmaatregelen

De Raad stelt, met gekwalificeerde meerderheid van stemmen en na raadpleging van het Europees Parlement, de maatregelen vast die nodig zijn voor de uitvoering van dit besluit op het niveau van de Unie.

([1]) PB L 281 van 23.11.1995, blz. 31. Richtlijn gewijzigd bij Verordening (EG) nr. 1882/2003 (PB L 284 van 31.10.2003, blz. 1).

Artikel 34

Kosten

Elke lidstaat draagt de operationele kosten die door zijn instanties bij de toepassing van dit besluit zijn gemaakt. In bijzondere gevallen kunnen de betrokken lidstaten een afwijkende regeling overeenkomen.

Artikel 35

Verhouding tot andere instrumenten

1. Voor de betrokken lidstaten zullen de desbetreffende bepalingen van dit besluit worden toegepast in de plaats van de overeenkomstige bepalingen in het Verdrag van Prüm. Elke andere bepaling van het Verdrag van Prüm blijft van toepassing tussen de verdragsluitende partijen.

2. Onverminderd hun verbintenissen uit hoofde van andere wetgevingsbesluiten die ingevolge titel VI van het Verdrag zijn aangenomen:

a) staat het de lidstaten vrij om bilaterale of multilaterale overeenkomsten of regelingen betreffende grensoverschrijdende samenwerking die van kracht zijn op het tijdstip van aanneming van dit besluit, te blijven toepassen, voor zover deze overeenkomsten of regelingen niet onverenigbaar zijn met de doelstellingen van dit besluit;

b) staat het de lidstaten vrij om bilaterale of multilaterale overeenkomsten of regelingen betreffende grensoverschrijdende samenwerking aan te gaan of in werking te doen treden nadat dit besluit van kracht is geworden, voor zover deze overeenkomsten of regelingen de mogelijkheid bieden de doelstellingen van dit besluit tussen de lidstaten te verruimen of te verbreden.

3. De in de leden 1 en 2 bedoelde overeenkomsten en regelingen laten de betrekkingen met de lidstaten die daarbij geen partij zijn, onverlet.

4. Binnen vier weken na het van kracht worden van dit besluit stellen de lidstaten de Raad en de Commissie in kennis van de bestaande overeenkomsten of regelingen in de zin van lid 2, onder a), die zij willen blijven toepassen.

5. De lidstaten stellen de Raad en de Commissie ook in kennis van iedere nieuwe overeenkomst of regeling in de zin van lid 2, onder b), binnen drie maanden na de ondertekening daarvan, dan wel, voor de instrumenten die reeds vóór de aanneming van dit besluit waren ondertekend, binnen drie maanden na de inwerkingtreding daarvan.

6. Dit besluit bevat geen bepalingen die afbreuk doen aan bilaterale of multilaterale overeenkomsten of regelingen tussen lidstaten en derde staten.

7. Dit besluit laat bestaande overeenkomsten betreffende rechtsbijstand of wederzijdse erkenning van rechterlijke beslissingen onverlet.

Artikel 36

Tenuitvoerlegging en verklaringen

1. De lidstaten nemen de nodige maatregelen om binnen een jaar na de inwerkingtreding aan dit besluit te voldoen, met uitzondering van de bepalingen van hoofdstuk 2, waarvoor de nodige maatregelen worden genomen binnen drie jaar na de inwerkingtreding van dit besluit en het besluit tot tenuitvoerlegging van dit besluit.

2. De lidstaten delen het secretariaat-generaal van de Raad en de Commissie mee dat zij aan de hun krachtens dit besluit opgelegde verplichtingen hebben voldaan en overleggen de in dit besluit bedoelde verklaringen. Bij deze mededeling kan iedere lidstaat laten weten dat hij dit besluit onmiddellijk zal toepassen in zijn betrekkingen met de lidstaten die dezelfde kennisgeving hebben gedaan.

3. De conform lid 2 ingediende verklaringen kunnen te allen tijde worden gewijzigd door middel van een bij het secretariaat-generaal van de Raad ingediende verklaring. Het secretariaat-generaal van de Raad zendt de ontvangen verklaringen door aan de lidstaten en de Commissie.

4. Op basis van deze en andere informatie die door de lidstaten op verzoek ter beschikking gesteld wordt, dient de Commissie uiterlijk op 28 juli 2012 bij de Raad een verslag in betreffende de tenuitvoerlegging van dit besluit, eventueel vergezeld van door haar passend geachte voorstellen voor vervolgstappen.

Artikel 37

Toepassing

Dit besluit treedt in werking twintig dagen volgende op die van zijn bekendmaking in het *Publicatieblad van de Europese Unie*.

Gedaan te Luxemburg, 23 juni 2008.

Voor de Raad

De voorzitter

I. JARC

BESLUIT 2008/616/JBZ VAN DE RAAD

van 23 juni 2008

betreffende de uitvoering van Besluit 2008/615/JBZ inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit

DE RAAD VAN DE EUROPESE UNIE,

Gelet op Besluit 2008/615/JBZ van de Raad en met name op artikel 33 [1],

Gezien het initiatief van de Bondsrepubliek Duitsland,

Gezien het advies van het Europees Parlement [2],

Overwegende hetgeen volgt:

(1) De Raad heeft op 23 juni 2008 Besluit 2008/615/JBZ inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit, aangenomen.

(2) Bij Besluit 2008/615/JBZ zijn de basiselementen van het Verdrag van 27 mei 2005 tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Franse Republiek, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie (hierna te noemen „het Verdrag van Prüm"), opgenomen in het rechtskader van de Europese Unie.

(3) In artikel 33 van Besluit 2008/615/JBZ is bepaald dat de Raad conform de procedure van artikel 34, lid 2, onder c), tweede zin, van het Verdrag betreffende de Europese Unie de maatregelen vaststelt die nodig zijn voor de uitvoering van Besluit 2008/615/JBZ op het niveau van de Unie. Deze maatregelen moeten worden gebaseerd op de Uitvoeringsovereenkomst van 5 december 2006 inzake de administratieve en technische uitvoering van het Verdrag van Prüm.

(4) Dit besluit bevat de gemeenschappelijke voorschriften voor de administratieve en technische uitvoering van de in Besluit 2008/615/JBZ vervatte samenwerkingsvormen. De bijlage bij dat besluit bevat uitvoeringsbepalingen van technische aard. Tevens zal een afzonderlijk handboek, met door de lidstaten te verstrekken zuiver feitelijke gegevens, door het secretariaat-generaal van de Raad worden opgesteld en geactualiseerd.

(5) Gezien de technische capaciteit geschiedt routinebevraging naar nieuwe DNA-profielen in beginsel bij wijze van enkelvoudige bevraging, waarvoor op technisch niveau passende oplossingen zullen worden gezocht,

BESLUIT:

HOOFDSTUK I

ALGEMEEN

Artikel 1

Doel

Dit besluit heeft ten doel de administratieve en technische bepalingen vast te stellen die nodig zijn ter uitvoering van Besluit 2008/615/JBZ, in het bijzonder voor de geautomatiseerde uitwisseling van DNA-gegevens, dactyloscopische gegevens en gegevens uit kentekenregisters, bedoeld in hoofdstuk 2, alsmede voor andere vormen van samenwerking, bedoeld in hoofdstuk 5.

Artikel 2

Begripsomschrijvingen

In dit besluit wordt verstaan onder:

a) „bevraging" en „vergelijking" in de zin van de artikelen 3, 4 en 9 van Besluit 2008/615/JBZ: de procedures aan de hand waarvan wordt vastgesteld of DNA-gegevens dan wel dactyloscopische gegevens die door een lidstaat worden verstrekt, overeenkomen met in de databank van één, meerdere of alle lidstaten opgeslagen DNA-gegevens of dactyloscopische gegevens;

b) „geautomatiseerde bevraging" in de zin van artikel 12 van Besluit 2008/615/JBZ: een online toegangsprocedure om de databanken van één, meerdere of alle lidstaten te raadplegen;

c) „DNA-profiel": een letter- of een cijfercode die een set identificatiekenmerken van het niet-coderende gedeelte van een geanalyseerd menselijk DNA-monster vertegenwoordigt, dat wil zeggen de specifieke moleculaire structuur op de verschillende DNA-gebieden (-loci);

d) „niet-coderende gedeelte van DNA": chromosoomgebieden die geen genetische uitdrukking bevatten, d.w.z. waarvan niet bekend is dat zij voorzien in functionele eigenschappen van een organisme;

[1] Zie bladzijde 1 van dit Publicatieblad.

[2] Advies van 21 april 2008 (nog niet bekendgemaakt in het Publicatieblad).

e) „DNA-linkgegevens": DNA-profiel en een kenmerk;

f) „DNA-persoonsprofiel": het DNA-profiel van een geïdentificeerd persoon;

g) „niet-geïdentificeerd DNA-profiel": een DNA-profiel dat uit tijdens het opsporingsonderzoek verzamelde sporen is verkregen en toebehoort aan een nog niet geïdentificeerd persoon;

h) „noot": een door een lidstaat in zijn nationale databank aangebrachte markering bij een DNA-profiel om aan te geven dat naar aanleiding van een bevraging of vergelijking door een andere lidstaat met betrekking tot dit DNA-profiel al een overeenkomst is vastgesteld;

i) „dactyloscopische gegevens": beelden van vingerafdrukken, van latente vingerafdrukken, van handpalmafdrukken en van latente handpalmafdrukken, alsook de sjablonen (templates) van die beelden (gecodeerde minutiae), welke zijn opgeslagen en behandeld in een geautomatiseerde databank;

j) „gegevens uit kentekenregisters": het geheel aan gegevens, gespecificeerd in hoofdstuk 3 van de bijlage;

k) „individueel geval" in de zin van artikel 3, lid 1, tweede zin, artikel 9, lid 1, tweede zin, en artikel 12, lid 1, van Besluit 2008/615/JBZ van de Raad: één enkel onderzoeks- of vervolgingsdossier. Indien het dossier meerdere DNA-profielen, dactyloscopische gegevens of gegevens uit een kentekenregister bevat, mogen deze gezamenlijk als één verzoek worden uitgewisseld.

HOOFDSTUK 2

GEMEENSCHAPPELIJKE BEPALINGEN VOOR GEGEVENSUITWISSELING

Artikel 3

Technische specificaties

De lidstaten nemen voor elk verzoek en antwoord met betrekking tot bevraging en vergelijking van DNA-profielen, dactyloscopische gegevens en gegevens uit kentekenregisters de gemeenschappelijke technische specificaties in acht. Deze technische specificaties staan in de bijlage.

Artikel 4

Communicatienetwerk

De elektronische uitwisseling van DNA-gegevens, dactyloscopische gegevens en gegevens uit kentekenregisters tussen de lidstaten geschiedt met gebruikmaking van het „Trans European Services for Telematics between Administrations" (TESTA II)-communicatienetwerk en verdere ontwikkelingen daarvan.

Artikel 5

Beschikbaarheid van geautomatiseerde gegevensuitwisseling

De lidstaten nemen alle nodige maatregelen om ervoor te zorgen dat de geautomatiseerde bevraging of vergelijking van DNA-gegevens, dactyloscopische gegevens of gegevens uit kentekenregisters dag en nacht mogelijk is. De nationale contactpunten van de lidstaten stellen elkaar onmiddellijk in kennis van technische mankementen, en komen conform de geldende regelgeving tijdelijke alternatieve regelingen voor gegevensuitwisseling overeen. De geautomatiseerde gegevensuitwisseling wordt zo spoedig mogelijk hervat.

Artikel 6

Kenmerk van DNA-gegevens en dactyloscopische gegevens

Het kenmerk, bedoeld in artikel 2 en artikel 8 van Besluit 2008/615/JBZ, bestaat uit een combinatie van:

a) een code die het de lidstaten mogelijk maakt om in geval van overeenkomende profielen persoonsgegevens en overige informatie uit hun databank te halen en overeenkomstig artikel 5 of artikel 10 van Besluit 2008/615/JBZ aan één, meerdere of alle lidstaten te verstrekken;

b) een code die de nationale oorsprong van het DNA-profiel of de dactyloscopische gegevens aanduidt, en

c) met betrekking tot DNA-gegevens, een code die het soort DNA-profiel aanduidt.

HOOFDSTUK 3

DNA-GEGEVENS

Artikel 7

Beginselen inzake de uitwisseling van DNA-gegevens

1. De lidstaten maken gebruik van bestaande standaarden voor de uitwisseling van DNA-gegevens zoals de „European Standard Set" (ESS) of de „Interpol Standard Set of Loci" (ISSOL).

2. Bij geautomatiseerde bevraging en vergelijking van DNA-profielen wordt de overdrachtprocedure in een decentrale structuur uitgevoerd.

3. De vertrouwelijkheid en de integriteit van naar andere lidstaten gezonden gegevens worden gegarandeerd door middel van passende maatregelen, waaronder versleuteling.

4. De lidstaten nemen de nodige maatregelen om de integriteit van beschikbaar gestelde of voor vergelijking aan de andere lidstaten toegezonden DNA-profielen te waarborgen en ervoor te zorgen dat de genomen maatregelen voldoen aan internationale normen zoals ISO 17025.

5. De lidstaten maken gebruik van lidstaatcodes conform ISO-norm 3166-1 alpha-2.

Artikel 8

Voorschriften inzake verzoek en antwoord betreffende DNA-gegevens

1. Het verzoek om geautomatiseerde bevraging of vergelijking in de zin van de artikelen 3 of 4 van Besluit 2008/615/JBZ bevat uitsluitend de volgende informatie:

a) de lidstaatcode van de verzoekende lidstaat;

b) de datum, de tijd en het verwijsnummer van het verzoek;

c) DNA-profielen en hun kenmerk;

d) de soorten DNA-profiel die worden overgedragen (niet-geïdentificeerde DNA-profielen of DNA-persoonsprofielen), en

e) de informatie die nodig is voor de besturing van de databanksystemen en de kwaliteitscontrole voor de geautomatiseerde bevragingsprocessen.

2. Het antwoord (matching report) op het verzoek, bedoeld in lid 1, bevat uitsluitend de volgende informatie:

a) de indicatie of er al dan niet sprake is van één of meerdere overeenkomende profielen (hit/no-hit);

b) de datum, de tijd en het verwijsnummer van het verzoek;

c) de datum, de tijd en het verwijsnummer van het antwoord;

d) de lidstaatcode van de verzoekende en van de aangezochte lidstaat;

e) het referentienummer van de verzoekende en van de aangezochte lidstaat;

f) het soort DNA-profiel dat wordt overgedragen (niet-geïdentificeerde DNA-profielen of DNA-persoonsprofielen);

g) de gevraagde en overeenstemmende DNA-profielen, en

h) de informatie die nodig is voor de besturing van de databanksystemen en de kwaliteitscontrole voor de geautomatiseerde bevragingsprocessen.

3. Er wordt alleen voorzien in geautomatiseerde melding van een overeenkomend profiel indien de geautomatiseerde bevraging of vergelijking een overeenkomst heeft opgeleverd voor een minimumaantal loci, dat in hoofdstuk 1 van de bijlage bij dit besluit is vastgesteld.

4. De lidstaten zorgen ervoor dat de verzoeken voldoen aan de verklaringen die conform artikel 2, lid 3, van Besluit 2008/615/JBZ worden afgelegd. Deze verklaringen worden opgenomen in het in artikel 18, lid 2, bedoelde handboek.

Artikel 9

Overdrachtprocedure voor de geautomatiseerde bevraging van niet-geïdentificeerde DNA-profielen overeenkomstig artikel 3 van Besluit 2008/615/JBZ

1. Indien er bij een bevraging op basis van een niet-geïdentificeerd DNA-profiel in de nationale databank geen overeenkomend profiel, of een overeenkomst met een niet-geïdentificeerd DNA-profiel is gevonden, kan het niet-geïdentificeerde DNA-profiel aan de databanken van alle andere lidstaten worden toegezonden; indien bij de bevraging op basis van dit niet-geïdentificeerde profiel in de databanken van andere lidstaten overeenkomsten worden gevonden met DNA-persoonsprofielen en/of met niet-geïdentificeerde DNA-profielen, worden deze overeenkomende profielen automatisch meegedeeld en worden de DNA-linkgegevens aan de verzoekende lidstaat toegezonden; indien er in de databanken van andere lidstaten geen overeenkomende profielen worden gevonden, wordt dit automatisch aan de verzoekende lidstaat meegedeeld.

2. Indien er bij een bevraging op basis van een niet-geïdentificeerd DNA-profiel in de databanken van andere lidstaten een overeenkomend profiel wordt gevonden, kan elke betrokken lidstaat dienaangaande een noot in zijn nationale databank opnemen.

Artikel 10

Overdrachtprocedure bij geautomatiseerde bevraging van DNA-persoonsprofielen overeenkomstig artikel 3 van Besluit 2008/615/JBZ

Indien er bij een bevraging op basis van een DNA-persoonsprofiel in de nationale databank geen overeenkomst met een DNA-persoonsprofiel, of een overeenkomst met een niet-geïdentificeerd DNA-profiel is gevonden, kan het DNA-persoonsprofiel aan de databanken van alle andere lidstaten worden toegezonden. Indien er bij een bevraging op basis van dit DNA-persoonsprofiel in de databanken van andere lidstaten overeenkomsten met DNA-persoonsprofielen en/of met niet-geïdentificeerde DNA-profielen worden gevonden, worden de overeenkomende profielen automatisch meegedeeld en worden de DNA-linkgegevens aan de verzoekende lidstaat toegezonden; indien er in de databanken van andere lidstaten geen overeenkomende profielen worden gevonden, wordt dit automatisch aan de verzoekende lidstaat meegedeeld.

Artikel 11

Overdrachtprocedure bij geautomatiseerde vergelijking van niet-geïdentificeerde DNA-profielen overeenkomstig artikel 4 van Besluit 2008/615/JBZ

1. Indien er bij een vergelijking op basis van niet-geïdentificeerde DNA-profielen in de databanken van andere lidstaten overeenkomsten met DNA-persoonsprofielen en/of met niet-geïdentificeerde DNA-profielen worden gevonden, worden de overeenkomende profielen automatisch meegedeeld en worden de DNA-linkgegevens aan de verzoekende lidstaat toegezonden.

2. Indien er bij een vergelijking op basis van niet-geïdentificeerde DNA-profielen in de databanken van andere lidstaten overeenkomsten met niet-geïdentificeerde DNA-profielen of met DNA-persoonsprofielen worden gevonden, kan elke betrokken lidstaat dienaangaande een noot in zijn nationale databank opnemen.

HOOFDSTUK 4

DACTYLOSCOPISCHE GEGEVENS

Artikel 12

Beginselen inzake de uitwisseling van dactyloscopische gegevens

1. Dactyloscopische gegevens worden gedigitaliseerd en aan de andere lidstaten verstrekt conform een uniform gegevensformaat, vastgesteld in hoofdstuk 2 van de bijlage.

2. Elke lidstaat ziet erop toe dat de dactyloscopische gegevens die hij verstrekt van een voldoende kwaliteit zijn voor een vergelijking door middel van het geautomatiseerde vingerafdrukidentificatiesysteem (AFIS).

3. De overdrachtprocedure voor de uitwisseling van dactyloscopische gegevens wordt in een decentrale structuur uitgevoerd.

4. Passende maatregelen, waaronder versleuteling, worden genomen om de vertrouwelijkheid en de integriteit van de gegevens te garanderen.

5. De lidstaten maken gebruik van lidstaatcodes conform ISO-norm 3166-1 alpha-2.

Artikel 13

Bevragingscapaciteit voor dactyloscopische gegevens

1. Elke lidstaat zorgt ervoor dat zijn bevragingsverzoeken de door de aangezochte lidstaat bepaalde bevragingscapaciteit niet overtreffen. De lidstaten doen in een verklaring overeenkomstig artikel 18, lid 2, aan het secretariaat-generaal van de Raad mededeling van hun maximale capaciteit per dag voor de dactyloscopische gegevens van geïdentificeerde personen en voor de dactyloscopische gegevens van nog niet geïdentificeerde personen.

2. Het maximumaantal te controleren kandidaten dat per bevraging wordt geaccepteerd, staat in hoofdstuk 2 van de bijlage.

Artikel 14

Voorschriften inzake verzoek en antwoord in verband met dactyloscopische gegevens

1. De aangezochte lidstaat controleert onverwijld de kwaliteit van de overgedragen dactyloscopische gegevens volgens een volledig geautomatiseerde procedure. Mochten de gegevens zich niet lenen voor geautomatiseerde vergelijking, dan stelt de aangezochte lidstaat de verzoekende lidstaat daarvan onverwijld in kennis.

2. De aangezochte lidstaat voert de bevraging uit in de volgorde waarin de verzoeken zijn ontvangen. Het verzoek wordt volgens een volledig geautomatiseerde procedure binnen 24 uur uitgevoerd. De verzoekende lidstaat kan, indien zijn nationale wetgeving dat voorschrijft, om een versnelde behandeling verzoeken; de aangezochte lidstaat geeft hieraan onverwijld gevolg. In geval van overmacht wordt de vergelijking onverwijld uitgevoerd zodra de belemmering is opgeheven.

HOOFDSTUK 5

GEGEVENS UIT KENTEKENREGISTERS

Artikel 15

Beginselen inzake geautomatiseerde bevraging van gegevens uit kentekenregisters

1. Voor de geautomatiseerde bevraging van gegevens uit kentekenregisters maken de lidstaten gebruik van een versie van de speciaal ten behoeve van artikel 12 van Besluit 2008/615/JBZ ontwikkelde softwaretoepassing EUCARIS (European Vehicle and Driving Licence Information System, Europees voertuig- en rijbewijsinformatiesysteem), en de gewijzigde versies daarvan.

2. De geautomatiseerde bevraging van gegevens uit kentekenregisters vindt binnen een decentrale structuur plaats.

3. De via het EUCARIS-systeem uitgewisselde informatie wordt in een versleutelde vorm overgedragen.

4. De uit te wisselen gegevenselementen uit kentekenregisters staan in hoofdstuk 3 van de bijlage.

5. De lidstaten kunnen bij de uitvoering van artikel 12 van Besluit 2008/615/JBZ van de Raad voorrang geven aan bevraging in verband met de bestrijding van zware criminaliteit.

Artikel 16

Kosten

Elke lidstaat draagt de kosten in verband met de administratie, het gebruik en het onderhoud van de in artikel 15, lid 1, vermelde softwaretoepassing EUCARIS.

HOOFDSTUK 6

POLITIËLE SAMENWERKING

Artikel 17

Gezamenlijke patrouilles en andere gezamenlijke operaties

1. Overeenkomstig hoofdstuk 5 van Besluit 2008/615/JBZ, met name in de in artikel 17, lid 4, en artikel 19, leden 2 en 4, van dat besluit bedoelde verklaringen, wijst elke lidstaat een of meer contactpunten aan waarlangs de andere lidstaten zich tot de

bevoegde autoriteiten kunnen richten, en kan elke lidstaat bepalen volgens welke procedures gezamenlijke patrouilles en andere gezamenlijke operaties worden opgezet en initiatieven van andere lidstaten aangaande die operaties hun beslag krijgen, andere praktische aspecten regelen en de operationele werkwijze vastleggen.

2. De lijst van contactpunten wordt opgesteld en bijgehouden door het secretariaat-generaal van de Raad, dat de bevoegde autoriteiten ook in kennis stelt van wijzigingen.

3. Het initiatief tot een gezamenlijke operatie kan uitgaan van de bevoegde autoriteiten van een lidstaat. Vóór de aanvang van de operatie maken de in lid 2 bedoelde bevoegde autoriteiten schriftelijk of mondeling afspraken over bijzonderheden zoals:

a) de voor de operatie bevoegde autoriteiten van de lidstaten;

b) het specifieke doel van de operatie;

c) de gastlidstaat waar de operatie plaatsvindt;

d) het geografische gebied van de gastlidstaat waarin de operatie plaatsvindt;

e) de periode waarop de operatie betrekking heeft;

f) de specifieke bijstand die de zendstaat (zendstaten) aan de gaststaat (gaststaten) verleent (verlenen), inclusief ambtenaren of ander overheidspersoneel, materiaal en financiële elementen;

g) de ambtenaren die deelnemen aan de operatie;

h) de ambtenaar die de leiding heeft over de operatie;

i) de bevoegdheden die ambtenaren en ander overheidspersoneel van de zendstaat(staten) in de gastlidstaat mogen uitoefenen gedurende de operatie;

j) de specifieke bewapening, munitie en uitrusting die de ondersteunende ambtenaren gedurende de operatie mogen gebruiken overeenkomstig Besluit 2008/615/JBZ;

k) de logistieke regelingen aangaande transport, accommodatie en beveiliging;

l) de verdeling van de kosten van de gezamenlijke operatie als wordt afgeweken van artikel 34, eerste zin, van Besluit 2008/615/JBZ;

m) andere mogelijk noodzakelijke elementen.

4. De in dit artikel bedoelde verklaringen, procedures en aanwijzingen worden opgenomen in het in artikel 18, lid 2, bedoelde handboek.

HOOFDSTUK 7

SLOTBEPALINGEN

Artikel 18

Bijlage en handboek

1. Nadere bijzonderheden betreffende de technische en administratieve uitvoering van Besluit 2008/615/JBZ staan in de bijlage.

2. Het secretariaat-generaal van de Raad stelt een handboek op dat uitsluitend feitelijke gegevens bevat, door de lidstaten verstrekt door middel van de verklaringen, bedoeld in Besluit 2008/615/JBZ en in het onderhavige besluit, of door middel van kennisgevingen aan het secretariaat-generaal van de Raad, en actualiseert dit handboek. Het handboek heeft de vorm van een Raadsdocument.

Artikel 19

Voor de gegevensbescherming bevoegde onafhankelijke instanties

Overeenkomstig artikel 18, lid 2, stellen de lidstaten het secretariaat-generaal van de Raad in kennis van hun voor de gegevensbescherming bevoegde onafhankelijke instanties of gerechtelijke autoriteiten in de zin van artikel 30, lid 5, van Besluit 2008/615/JBZ.

Artikel 20

Voorbereiding van de in artikel 25, lid 2, van Besluit 2008/615/JBZ bedoelde besluiten

1. De Raad neemt het in artikel 25, lid 2, van Besluit 2008/615/JBZ bedoelde besluit op basis van een evaluatieverslag, dat is opgesteld aan de hand van een vragenlijst.

2. Met betrekking tot de geautomatiseerde uitwisseling van gegevens in de zin van hoofdstuk 2 van Besluit 2008/615/JBZ wordt het evaluatieverslag tevens gebaseerd op een evaluatiebezoek en een proefrun die plaatsvindt na de mededeling van de betrokken lidstaat aan het secretariaat-generaal van de Raad, bedoeld in artikel 36, lid 2, eerste zin, van Besluit 2008/615/JBZ.

3. De procedure is nader geregeld in hoofdstuk 4 van de bijlage.

Artikel 21

Evaluatie van de gegevensuitwisseling

1. De administratieve, technische en financiële toepassing van de gegevensuitwisseling in de zin van hoofdstuk 2 van Besluit 2008/615/JBZ, met name het gebruik van het in artikel 15, lid 5, bedoelde mechanisme worden op gezette tijden geëvalueerd. De evaluatie heeft betrekking op de lidstaten die op het tijdstip van de evaluatie Besluit 2008/615/JBZ al toepassen en op de

gegevenscategorieën waarvoor de uitwisseling tussen deze lidstaten al begonnen is. De evaluatie wordt gebaseerd op verslagen van de betrokken lidstaten.

2. De procedure is nader geregeld in hoofdstuk 4 van de bijlage.

Artikel 22

Samenhang met de Uitvoeringsovereenkomst van het Verdrag van Prüm

Voor de door het Verdrag van Prüm gebonden lidstaten treden de desbetreffende bepalingen van dit besluit en de bijlage, wanneer zij volledig in werking zijn getreden, in de plaats van de overeenkomstige bepalingen van de Uitvoeringsovereenkomst van het Verdrag van Prüm. Elke andere bepaling van de Uitvoeringsovereenkomst blijft van toepassing tussen de partijen bij het Verdrag van Prüm.

Artikel 23

Uitvoering

De lidstaten nemen de nodige maatregelen om binnen de in artikel 36, lid 1, van Besluit 2008/615/JBZ bedoelde termijnen aan de bepalingen van het onderhavige besluit te voldoen.

Artikel 24

Toepassing

Dit besluit treedt in werking twintig dagen na de dag van zijn bekendmaking in het *Publicatieblad van de Europese Unie*.

Gedaan te Luxemburg, 23 juni 2008.

Voor de Raad

De voorzitter

I. JARC

BIJLAGE

INHOUD

HOOFDSTUK 1: **Uitwisseling van DNA-gegevens**

1. ***DNA: forensische aspecten, matchingregels en algoritmen***

1.1. *Kenmerken van DNA-profielen*

DNA-profielen kunnen uit 24 nummerparen bestaan, die de allelen van de 24 loci voorstellen die ook in de DNA-procedures van Interpol worden gebruikt. De namen van deze loci zijn:

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

De 7 grijze loci in de bovenste rij vormen zowel de huidige European Standard Set (ESS — Europese Standaard Set) als de Interpol standaard locireeks (ISSOL).

Opnameregels:

Wanneer de lidstaten DNA-profielen ter beschikking stellen voor bevragingen of vergelijkingen, of wanneer DNA-profielen voor dat doel worden verzonden, moeten deze ten minste 6 volledig toegewezen ([1]) loci bevatten; de DNA-profielen kunnen ook aanvullende loci of blanco's bevatten, voor zover deze beschikbaar zijn. Referentie-DNA-profielen moeten ten minste 6 van de 7 ESS-loci bevatten. Voor een grotere accuraatheid van de overeenkomsten worden alle beschikbare allelen opgeslagen in de geïndexeerde databank van DNA-profielen en voor bevragingen en vergelijkingen gebruikt. De lidstaten dienen iedere door de Europese Unie aangenomen nieuwe ESS-locus zo spoedig als praktisch mogelijk toe te passen.

Gemengde profielen worden niet aanvaard. De allelwaarden van elke locus bestaan bijgevolg uit slechts 2 cijfers; in het geval van homozygositeit op een bepaalde locus kunnen dit dezelfde cijfers zijn.

Wild cards en microvarianten moeten als volgt worden behandeld:

— Alle niet-numerieke waarden in het profiel (bv. „o", „f", „r", „na", „nr" of „un"), met uitzondering van amelogenine, moeten automatisch worden geconverteerd naar een wild card (*) zodat ze met alle allelwaarden matchen.

— De numerieke waarden „0", „1" of „99" in een profiel moeten automatisch worden geconverteerd in een wild card (*) zodat ze met alle allelwaarden matchen.

— Indien voor één locus 3 allelen worden aangeleverd, wordt het eerste allel aanvaard en moeten de 2 andere allelen automatisch worden geconverteerd naar een wild card (*) zodat ze met alle allelwaarden matchen.

— Wanneer voor het eerste of het tweede allel wild card-waarden worden aangeleverd, wordt een bevraging verricht voor de beide permutaties van de numerieke waarde voor de betreffende locus (bv. 12, * zou kunnen matchen met 12,14 of 9,12).

— Microvarianten van penta-nucleotide (Penta D, Penta E & CD4) worden als volgt „gematched":

  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

— Microvarianten van tetra-nucleotide (alle overige loci zijn tetra-nucleotiden) worden als volgt „gematched":

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

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

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

([1]) „Volledig toegewezen" betekent dat ook de zeldzame allelwaarden worden meegenomen.

1.2. *Matchingregels*

Het vergelijken van 2 DNA-profielen gebeurt op basis van de loci waarvoor in de beide DNA-profielen een paar allelwaarden beschikbaar is. Tussen de beide DNA-profielen moet er een overeenkomst van ten minste 6 volledig toegewezen loci (amelogenine niet meegerekend) zijn alvorens een „hit" wordt gemeld.

Onder een volledige overeenkomst („full match") (kwaliteit 1) wordt verstaan, een overeenkomst waarbij alle allelwaarden van de vergeleken loci die het bevragende én het bevraagde DNA-profiel gemeenschappelijk hebben, gelijk zijn. Een bijna-overeenkomst („near match") wordt omschreven als een overeenkomst waarbij van slechts één van alle vergeleken allelen in de twee DNA-profielen de waarde anders is (kwaliteit 2, 3 en 4). Een bijna-overeenkomst wordt alleen aanvaard indien er in de twee vergeleken DNA-profielen voor ten minste 6 volledig toegewezen loci een volledige overeenkomst is.

Een bijna-overeenkomst kan het gevolg zijn van:

— een menselijke typefout bij het invoeren van een van de DNA-profielen in de zoekopdracht of in de DNA-databank;

— een fout bij het herkennen of benoemen van een allel tijdens het genereren van een DNA-profiel.

1.3. *Rapporteringsregels*

Volledige overeenkomsten, bijna-overeenkomsten en „geen overeenkomsten" worden gerapporteerd.

Het match-rapport wordt aan het verzoekende nationaal contactpunt toegezonden en wordt tevens ter beschikking gesteld van het aangezochte nationaal contactpunt (zodat het een raming kan maken van de aard en het aantal mogelijke daaropvolgende verzoeken om andere beschikbare persoonsgegevens en andere informatie in verband met het DNA-profiel dat overeenkomt met de „hit" overeenkomstig de artikelen 5 en 10 van Besluit 2008/615/JBZ).

2. ***Codes lidstaten (tabel)***

Overeenkomstig Besluit 2008/615/JBZ wordt ISO-code 3166-1 alfa-2 gebruikt voor de domeinnamen en andere configuratieparameters die noodzakelijk zijn in de applicaties voor het uitwisselen van DNA-gegevens over een gesloten netwerk in het kader van het Verdrag van Prüm.

De ISO-codes 3166-1 alfa-2 komen overeen met de volgende tweelettercodes voor de lidstaten:

Naam lidstaat	Code	Naam lidstaat	Code
België	BE	Luxemburg	LU
Bulgarije	BG	Hongarije	HU
Tsjechië	CZ	Malta	MT
Denemarken	DK	Nederland	NL
Duitsland	DE	Oostenrijk	AT
Estland	EE	Polen	PL
Griekenland	EL	Portugal	PT
Spanje	ES	Roemenië	RO
Frankrijk	FR	Slowakije	SK
Ierland	IE	Slovenië	SI
Italië	IT	Finland	FI
Cyprus	CY	Zweden	SE
Letland	LV	Verenigd Koninkrijk	UK
Litouwen	LT		

3. ***Functionele analyse***

3.1. *Beschikbaarheid van het systeem*

Verzoeken op grond van artikel 3 van Besluit 2008/615/JBZ moeten in de chronologische volgorde waarin ieder verzoek werd verstuurd in de doeldatabank worden ontvangen; antwoorden dienen de verzoekende lidstaten binnen 15 minuten na binnenkomst van het verzoek te bereiken.

3.2. *Tweede stap*

Wanneer een lidstaat een „match"-bericht ontvangt, dient zijn nationaal contactpunt de waarden van het verzoekprofiel te vergelijken met de waarden van het (de) antwoordprofiel(en) teneinde de bewijswaarde van het profiel te valideren en te controleren. De nationale contactpunten kunnen rechtstreeks met elkaar contact opnemen voor het valideren van profielen.

Rechtshulpprocedures gaan pas van start nadat een bestaande overeenkomst tussen twee profielen is gevalideerd, op basis van een „volledige overeenkomst" of een „bijna-overeenkomst" die de geautomatiseerde raadpleging heeft opgeleverd.

4. ***DNA-interfacecontroledocument***

4.1. *Inleiding*

4.1.1. Doelstellingen

In dit hoofdstuk wordt bepaald aan welke eisen de uitwisseling van DNA-profielgegevens tussen de DNA-databanken van de lidstaten moet voldoen. De bestandsaanhefvelden zijn specifiek gedefinieerd voor het uitwisselen van DNA-gegevens in het kader van het Verdrag van Prüm, terwijl het gegevensgedeelte gebaseerd is op dat van de DNA-profielgegevens in het XML-schema dat voor de Interpol-gateway voor de uitwisseling van DNA-gegevens is gedefinieerd.

De gegevens worden uitgewisseld via een SMTP (Simple Mail Transfer Protocol) en andere geavanceerde technologieën, door middel van een centrale relay-mailserver van de netwerkaanbieder. Het XML-bestand wordt in het tekstgedeelte verstuurd.

4.1.2. Werkingssfeer

In dit interfacecontroledocument wordt alleen de inhoud van het bericht (mail) gedefinieerd. Alle netwerkspecifieke en mailspecifieke aspecten worden op uniforme wijze gedefinieerd, zodat een gemeenschappelijke technische basis voor het uitwisselen van DNA-gegevens ontstaat.

Dit omvat het volgende:

— het formaat van het onderwerpveld in het bericht, zodat de berichten automatisch kunnen/mogen worden verwerkt;

— eventuele versleuteling van de inhoud en, in dat geval, de methoden die daarvoor moeten worden gekozen;

— de maximale lengte van de berichten.

4.1.3. XML-structuur en -beginselen

De structuur van het XML-bericht ziet er als volgt uit:

— aanhefgedeelte, met informatie over de transmissie, en

— gegevensgedeelte, met profielspecifieke informatie en het profiel zelf.

Voor verzoeken en antwoorden wordt hetzelfde XML-schema gebruikt.

In één bericht moet er een hele reeks profielen kunnen worden verstuurd, zodat niet-geïdentificeerde DNA-profielen aan een volledige controle kunnen worden onderworpen (artikel 4 van Besluit 2008/615/JBZ). Er moet een maximum worden vastgesteld voor het aantal profielen in één bericht. Het aantal hangt af van de toegestane maximumgrootte van het bericht en wordt vastgesteld nadat de mailserver is geselecteerd.

XML-voorbeeld:

<?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> datastructuur wordt herhaald indien er meerdere profielen in één SMTP-(....) bericht worden verzonden; alleen toegestaan voor artikel 4-gevallen

</datas>]

</PRUEMDNA>

4.2. *Definitie XML-structuur*

De volgende definities zijn bedoeld als documentatie en voor een beter begrip; de echte, bindende informatie wordt verstrekt door middel van een XML-schemabestand (PRUEM DNA.xsd).

4.2.1. Schema PRUEMDNAx

Dit bevat de volgende velden:

Velden	Type	Omschrijving
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 ... 500

4.2.2. Inhoud van de aanhefstructuur

4.2.2.1. PRUEM header

In deze structuur wordt de aanhef van het XML-bestand beschreven. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
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

Soort gegevens in het bericht; de waarde hiervan kan zijn:

Waarde	Omschrijving
R	Request

Waarde	Omschrijving
A	Answer

4.2.2.3. PRUEM header info

Structuur ter aanduiding van de lidstaat en van de datum/het tijdstip van het bericht. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
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. Inhoud van de PRUEM Profile-gegevens

4.2.3.1. PRUEM_datas

In deze structuur wordt het gedeelte van de XML-profielgegevens beschreven. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
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

Soort gegevens in het bericht; de waarde hiervan kan zijn:

Waarde	Omschrijving
3	Requests pursuant to Article 3 of Decision 2008/615/JHA
4	Requests pursuant to Article 4 of Decision 2008/615/JHA

4.2.3.3. PRUEM_hitquality_type

Waarde	Omschrijving
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

Soort gegevens in het bericht; de waarde hiervan kan zijn:

Waarde	Omschrijving
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

Soort gegevens in het bericht; de waarde hiervan kan zijn:

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

4.2.3.6. IPSG_DNA_profile

Structuur waarmee een DNA-profiel wordt beschreven. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
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

Structuur die de ISSOL-loci (standaardgroep van Interpol-loci) bevat. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Velden	Type	Omschrijving
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

Structuur die de andere loci bevat. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
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

Structuur waarmee een locus wordt beschreven. Dit gedeelte bevat de volgende velden:

Velden	Type	Omschrijving
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. *Applicatie-, beveiligings- en communicatiearchitectuur*

5.1. *Overzicht*

Voor het afhandelen van verzoeken tot uitwisseling van DNA-gegevens in het kader van Besluit 2008/615/JBZ moet een gemeenschappelijk, logisch gesloten communicatienetwerk tussen de lidstaten worden gebruikt. Om deze gemeenschappelijke communicatie-infrastructuur voor het verzenden van verzoeken en ontvangen van

antwoorden efficiënter te benutten, is gekozen voor een asynchroon mechanisme voor het versturen van verzoeken om DNA- en dactyloscopische gegevens, in de vorm van een „verpakt" SMTP e-mailbericht. Om tegemoet te komen aan de beveiligingseisen zal het sMIME-mechanisme (Secure/Multipurpose Internet Mail Extensions) worden gebruikt als extensie van het SMTP (Simple Mail Transfer Protocol), zodat een werkelijk veilige tunnel (eind-tot-eind) over het netwerk tot stand kan worden gebracht.

Als communicatienetwerk voor de uitwisseling van gegevens tussen de lidstaten wordt het reeds operationele TESTA (Trans European Services for Telematics between Administrations) gebruikt. TESTA ressorteert onder de verantwoordelijkheid van de Commissie. Aangezien de nationale DNA-databanken en de huidige nationale TESTA-toegangspunten zich op verschillende sites in de lidstaten kunnen bevinden, kan de toegang tot TESTA tot stand worden gebracht door:

1. gebruik te maken van het bestaande nationale toegangspunt of een nieuw nationaal TESTA-toegangspunt te creëren, of door

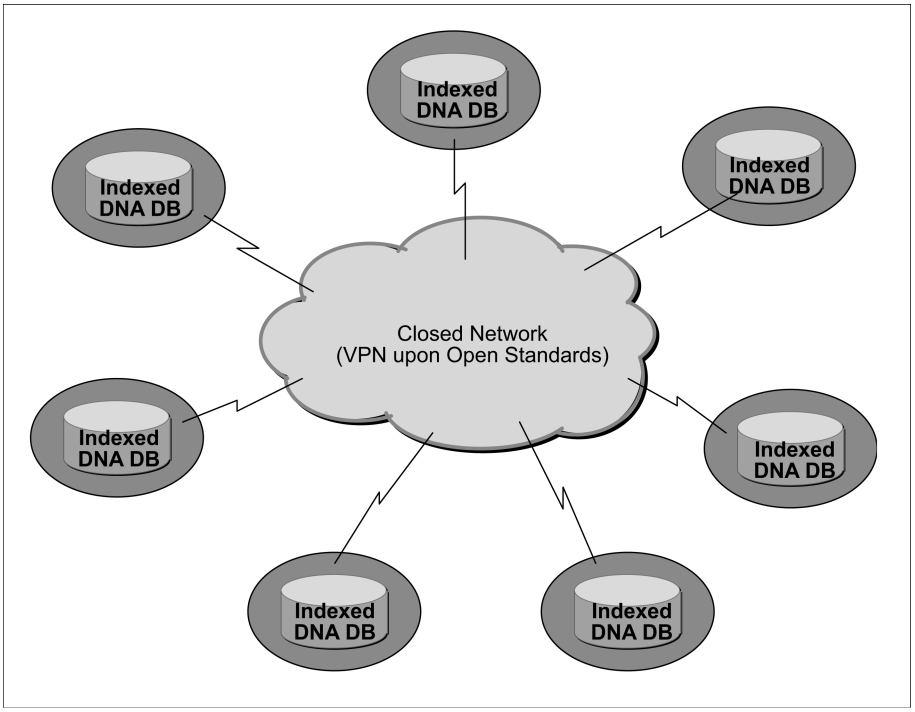
2. een beveiligde lokale verbinding tot stand te brengen tussen de door de bevoegde nationale dienst beheerde site van de DNA-databank en het bestaande nationale TESTA-toegangspunt.

De protocollen en normen voor applicaties die ter uitvoering van Besluit 2008/615/JBZ worden gebruikt, voldoen aan de open normen en beantwoorden aan de eisen van de nationale beveiligingsvoorschriften van de lidstaten.

5.2. *Architectuur centrale niveau*

In het kader van Besluit 2008/615/JBZ stellen de lidstaten hun DNA-databanken open voor uitwisselingen met en/of bevragingen van andere lidstaten volgens het gestandaardiseerde gemeenschappelijke dataformaat. De architectuur is gebaseerd op een zogeheten „any-to-any"-communicatiemodel. Er is geen centrale computerserver en ook geen centrale databank waarin DNA-profielen worden bewaard.

Figuur 1: Schematische voorstelling van de uitwisseling van DNA-gegevens



Afgezien van de nationale wettelijke voorschriften waaraan de sites van de lidstaten moeten voldoen, kunnen de lidstaten bepalen welke hardware en software moeten worden gebruikt om hun siteconfiguraties te laten voldoen aan de eisen van Besluit 2008/615/JBZ.

5.3. *Beveiligingsnormen en gegevensbescherming*

Er zijn drie beveiligingsniveaus onderzocht en geïmplementeerd.

5.3.1. Gegevensniveau

De DNA-profielgegevens die de lidstaten verstrekken, moeten aan een gemeenschappelijke gegevensbeschermingsnorm voldoen, zodat de verzoekende lidstaat in eerste instantie als antwoord de melding „HIT" of „NO HIT" ontvangt, tezamen met — in het geval van een „HIT" — een identificatienummer dat geen persoonsgegevens bevat. Verder onderzoek na een HIT-melding wordt op bilateraal niveau uitgevoerd, met inachtneming van de nationale wettelijke en organisatorische voorschriften die gelden voor de sites van de respectieve lidstaten.

5.3.2. Communicatieniveau

Berichten die informatie over DNA-profielen bevatten (verzoeken en antwoorden), worden versleuteld door middel van de nieuwste mechanismen en volgens open normen, zoals sMIME, alvorens deze naar de sites van andere lidstaten worden verzonden.

5.3.3. Transmissieniveau

Versleutelde berichten met informatie over DNA-profielen worden door een virtueel gesloten tunnelsysteem naar de sites van de andere lidstaten verstuurd. Dit systeem wordt op internationaal niveau door een erkende netwerkaanbieder beheerd; de beveiligde verbindingen met dit tunnelsysteem vallen onder de nationale verantwoordelijkheid. Dit virtuele gesloten tunnelsysteem heeft geen connectiepunt met het open internet.

5.4. *Protocollen en normen voor het versleutelingsmechanisme: sMIME en aanverwante pakketten*

Voor de versleuteling van berichten met informatie over DNA-profielen zal gebruik worden gemaakt van de open norm sMIME als uitbreiding van SMTP (de feitelijke e-mailnorm). Het sMIME-protocol (V3) staat getekende ontvangstmeldingen, veiligheidslabels en beveiligde mailinglijsten toe en berust op een zogeheten Cryptographic Message Syntax (CMS), een IETF-specificatie voor berichten met beveiligingsversleuteling. Het kan worden gebruikt om digitale gegevens, ongeacht hun vorm, digitaal te ondertekenen, te systematiseren, te authenticeren of te versleutelen.

Het onderliggende certificaat dat door het sMIME-mechanisme wordt gebruikt, moet voldoen aan de X.509-norm. Met het oog op gemeenschappelijke normen en procedures met andere Prüm-applicaties zien de verwerkingsregels voor sMIME-versleutelingsoperaties, c.q. de regels die in verschillende COTS-omgevingen (Commercial Product of the Shelves — commercieel standaardproduct) moeten worden toegepast, er als volgt uit:

— De sequentie is eerst versleuteling en nadien ondertekening.

— Voor symmetrische versleuteling wordt een AES-versleutelingsalgoritme (Advanced Encryption Standard) met een sleutellengte van 256 bits gebruikt, en voor asymmetrische versleuteling een RSA-algoritme met een sleutellengte van 1 024 bits.

— Er wordt gebruikgemaakt van de hash-algoritme SHA-1.

Nagenoeg alle moderne e-mailsoftwarepakketten, zoals Outlook, Mozilla Mail en Netscape Communicator 4.x, bevatten de functie sMIME, die verenigbaar is met alle grote softwarepakketten voor elektronisch berichtenverkeer.

Voor de implementatie van het communicatiebeveiligingsniveau is gekozen voor sMIME, omdat dit gemakkelijk in de nationale IT-infrastructuur van de sites van de lidstaten kan worden geïntegreerd en bijgevolg een haalbaar mechanisme is. Om efficiënter en met minder kosten de beoogde „Proof of Concept"-doelstelling te kunnen halen, is evenwel voor de open norm JavaMail API gekozen voor het uitwerken van een prototype voor de uitwisseling van DNA-gegevens. JavaMail API biedt een eenvoudige versleuteling en ontsleuteling van e-mailberichten aan door middel van s/MIME en/of OpenPGP. Het is de bedoeling één enkele gebruiksvriendelijke API aan te bieden aan e-mailgebruikers die versleutelde berichten wensen te versturen en te ontvangen in een van de twee meest gebruikte formaten voor het versleutelen van e-mailberichten. Voor de in Besluit 2008/615/JBZ vastgelegde eisen zullen bijgevolg de nieuwste implementaties van JavaMail API volstaan, zoals het Bouncy Castle-product JCE (Java Cryptographic Extension), dat zal worden gebruikt voor het implementeren van sMIME met het oog op de uitwerking van een prototype voor de uitwisseling van DNA-gegevens tussen de lidstaten.

5.5. *Applicatiearchitectuur*

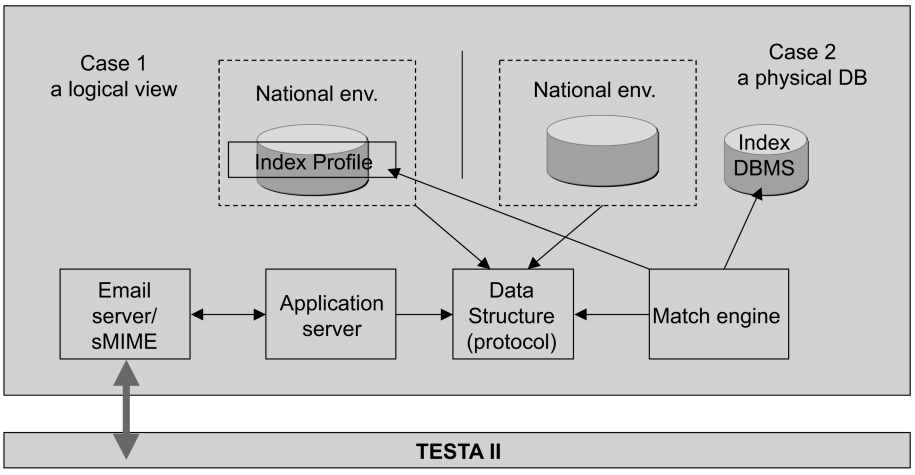
Elke lidstaat bezorgt de andere lidstaten een reeks gestandaardiseerde DNA-profielgegevens die beantwoorden aan het huidige gemeenschappelijk interfacecontroledocument. Daartoe kan een logische „view" voor een bepaalde nationale databank tot stand worden gebracht of een fysiek geëxporteerde databank (geïndexeerde databank) worden gecreëerd.

De volledige applicatielogica wordt door de vier belangrijkste componenten — de e-mailserver/sMIME, de applicatieserver, het datastructuurdomein voor de data fetching/feeding en het registreren van binnenkomende/uitgaande berichten, en de „match engine" — op een productonafhankelijke manier geïmplementeerd.

Om ervoor te zorgen dat alle lidstaten de componenten gemakkelijk in hun respectieve nationale sites kunnen integreren, is de gespecificeerde gemeenschappelijke functie geïmplementeerd door middel van componenten uit open bronnen, die de lidstaten afhankelijk van hun nationaal IT-beleid en hun regelgeving ter zake kunnen kiezen. Voor het verlenen van toegang tot geïndexeerde databanken van DNA-profielen die vallen onder Besluit 2008/615/JBZ moeten onafhankelijke voorzieningen worden geïmplementeerd; daarom kunnen de lidstaten hun hardware- en softwareplatform, met inbegrip van de databank- en besturingssystemen, vrij kiezen.

Er is een prototype voor de uitwisseling van DNA-gegevens ontwikkeld, dat met succes is getest in het bestaande gemeenschappelijk netwerk. Versie 1.0 is ingezet in de productieomgeving en wordt voor dagelijkse operaties gebruikt. De lidstaten kunnen gebruikmaken van het gemeenschappelijk ontwikkelde product, maar kunnen ook eigen producten ontwikkelen. Al naargelang de veranderende IT-, forensische en/of functionele beleidseisen zullen de gemeenschappelijke productcomponenten worden behouden, aangepast of verder ontwikkeld.

Figuur 2: Overzicht van de eigenschappen van de applicatie



5.6. *Protocollen en normen voor de applicatiearchitectuur*

5.6.1. XML

Voor de uitwisseling van DNA-gegevens wordt volledig gebruikgemaakt van het XML-schema, als attachment bij SMTP e-mailberichten. XML (eXtensible Markup Language) is een door het World Wide Web Consortium (W3C) aanbevolen algemene markeertaal die wordt gebruikt voor het creëren van markeertalen voor bijzondere doeleinden, waarmee vele verschillende soorten gegevens kunnen worden beschreven. DNA-profielen die voor uitwisseling tussen de lidstaten in aanmerking komen, zijn in het interfacecontroledocument door middel van XML en XML-schema beschreven.

5.6.2. ODBC

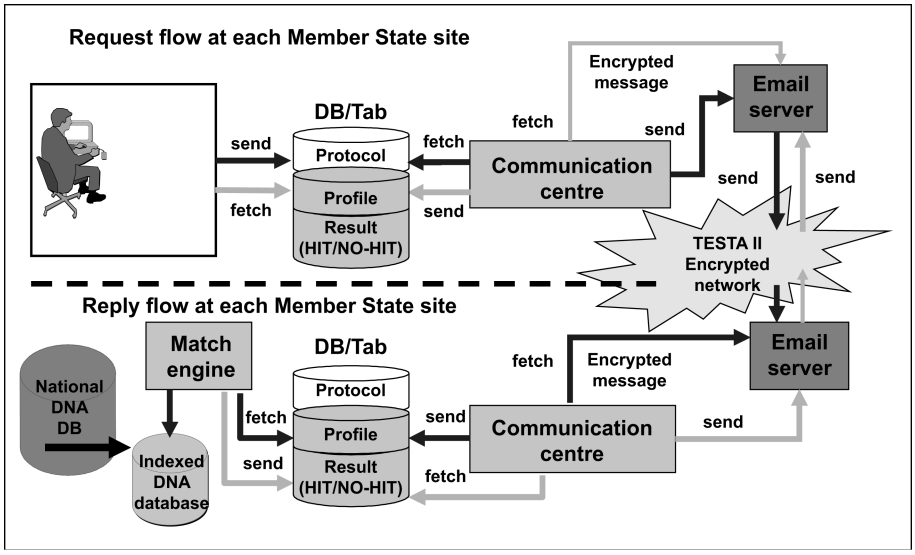
ODBC (Open DataBase Connectivity) is een standaard programmeerinterfacemethode voor softwareapplicaties die wordt gebruikt om toegang te verlenen tot databankbeheersystemen en om deze onafhankelijk te maken van programmeertalen, databank- en besturingssystemen. ODBC heeft echter bepaalde nadelen. Het beheer van een groot aantal gebruikersmachines kan tot een grote verscheidenheid aan drivers en DLL's zorgen. Door deze complexiteit kunnen de algemene kosten van het systeembeheer toenemen.

5.6.3. JDBC

JDBC (Java DataBase Connectivity) is een applicatieprogrammeerinterface voor de programmeertaal Java waarbij wordt gedefinieerd op welke manier een gebruiker („cliënt") toegang kan krijgen tot een databank. Anders dan voor ODBC, hoeven voor JDBC geen lokale DLL's op de gebruikersmachine te worden gebruikt.

De logica voor het verwerken van verzoeken om DNA-profielen, en de antwoorden daarop, in de sites van de lidstaten wordt in het onderstaande diagram beschreven. Zowel de verzoeken- als de antwoordenstroom interageert met een neutrale datazone die bestaat uit verschillende datagehelen met een gemeenschappelijke datastructuur.

Figuur 3: Overzicht van de applicatieworkflow in de sites van de lidstaten



5.7. *Communicatieomgeving*

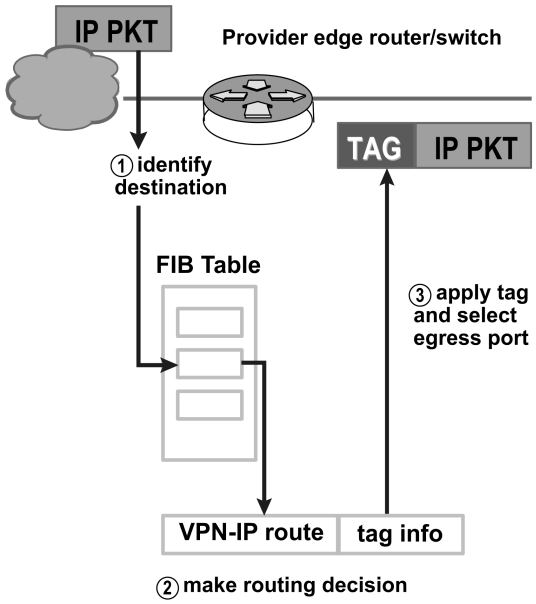
5.7.1. Gemeenschappelijk communicatienetwerk: TESTA en de follow-up-infrastructuur ervan

De applicatie voor het uitwisselen van DNA-gegevens zal het e-mailsysteem, een asynchroon mechanisme, gebruiken om tussen de lidstaten verzoeken te verzenden en antwoorden te ontvangen. Aangezien alle lidstaten over ten minste één nationaal TESTA-toegangspunt beschikken, zullen de DNA-gegevens in het TESTA-netwerk worden uitgewisseld. TESTA biedt een aantal meerwaardediensten door de bijbehorende e-mail relay. De infrastructuur biedt niet alleen specifieke TESTA-e-mailpostbussen, maar is ook geschikt voor het implementeren van maildistributielijsten en routingmaatregelen. Daardoor kan TESTA worden gebruikt als „clearing house" voor berichten die bestemd zijn voor overheidsdiensten die met EU-domeinen zijn verbonden. Er kan ook in viruscontrole worden voorzien.

De TESTA e-mail relay is gebouwd op een hardwareplatform met een hoge beschikbaarheidsgraad dat zich in de centrale applicatie van TESTA bevindt en door een firewall wordt beschermd. De Domain Name Services (domeinnaamdiensten — DNS) van TESTA zetten URL's om in IP-adressen en verbergen adresinformatie voor de gebruiker en applicaties.

5.7.2. Beveiliging

Het VPN-concept (virtueel gesloten netwerk) is al geïmplementeerd in het kader van TESTA. De Tag Switching Technology die is gebruikt om dit VPN tot stand te brengen, zal verder worden uitgebouwd om de MPLS-norm (Multi-Protocol Label Switching) te ondersteunen die door de Internet Engineering Task Force (IETF) is ontwikkeld.



MPLS is een IETF-standaardtechnologie die voor snellere netwerkverkeersstromen zorgt doordat pakketanalyses door tussenliggende routers (zogeheten „hops") worden voorkomen. Daartoe worden door de eindrouters van de verbindingen zogeheten labels aan het pakket gekoppeld, op basis van de informatie die wordt opgeslagen in de forwarding information base (FIB). Labels worden ook gebruikt om virtuele gesloten netwerken te implementeren.

MPLS combineert de voordelen van drielagen-routing met die van tweelagen-switching. Aangezien internetadressen niet worden geëvalueerd tijdens de transitie door de netwerkverbindingen houdt MPLS op dit punt geen beperkingen in.

E-mailberichten die met gebruikmaking van TESTA worden verzonden, worden bovendien beveiligd door het sMIME-versleutelingsmechanisme. Zonder kennis van de sleutel en zonder het juiste certificaat kunnen over het netwerk verzonden berichten niet worden ontsleuteld.

5.7.3. Protocollen en normen voor het communicatienetwerk

5.7.3.1. SMTP

SMPT (Simple Mail Transfer Protocol) is de feitelijke norm voor de transmissie van elektronische post over het internet. SMTP is een vrij eenvoudig, op tekst gebaseerd protocol waarbij eerst een of meer ontvangers van een bericht worden gespecificeerd en vervolgens de tekst wordt verstuurd. SMTP maakt gebruik van TCP-poort 25, die door de IETF is gespecificeerd. Om de SMTP-server voor een bepaalde domeinnaam vast te stellen, wordt gebruikgemaakt van een DNS-record (Domain Name System — domeinnamenstelsel) voor MX (Mail eXchange — berichtenuitwisseling).

Dit protocol was aanvankelijk uitsluitend op ASCII-tekst gebaseerd en voldeed daarom niet voor binaire bestanden. Dit heeft geleid tot de ontwikkeling van normen zoals MIME voor het encoderen van binaire bestanden zodat deze via SMTP kunnen worden verzonden. De meeste SMTP-servers ondersteunen thans de 8 bit MIME- en sMIME-extensie, waardoor binaire bestanden bijna net zo gemakkelijk kunnen worden verzonden als niet-gecodeerde tekst. De verwerkingsregels voor sMIME-operaties worden beschreven in het deel „sMIME" (zie hoofdstuk 5.4).

SMTP is een zogeheten „push"-protocol, waardoor berichten niet, wanneer iemand dat zou willen, via een server op afstand kunnen worden opgehaald („to pull"). Daarvoor moet een e-mailcliënt POP3 (Post Office Protocol, 3e versie) of IMAP (Internet Message Access Protocol) gebruiken. Er is besloten om het POP3-protocol te gebruiken voor het uitwisselen van DNA-gegevens.

5.7.3.2. POP

Lokale e-mailcliënten gebruiken de derde versie van het Post Office Protocol (POP3), een internetstandaardprotocol op het niveau van de applicatielaag, om e-mailberichten via een TCP/IP-verbinding op te halen van een server op afstand. Wanneer e-mailcliënten gebruikmaken van het SMTP Submit-profiel van het SMTP-protocol, verzenden zij berichten over het internet of over een intranet. MIME fungeert als norm voor attachments en voor niet-ASCII-tekst in e-mailberichten. Hoewel noch voor POP3 noch voor SMTP e-mailberichten in MIME-formaat vereist zijn, hebben de meeste e-mailberichten over het internet een MIME-formaat, hetgeen tot gevolg heeft dat ook POP-cliënten bekend moeten zijn met MIME en het moeten gebruiken. De volledige communicatieomgeving van Besluit 2008/615/JBZ zal derhalve de POP-componenten bevatten.

5.7.4. Toewijzing van netwerkadressen

Operationele omgeving

De Europese IP-registratieautoriteit (RIPE) heeft aan TESTA een specifiek deel van een C-klasse-subnet toegewezen. Indien nodig kunnen in de toekomst nog meer adresblokken aan TESTA worden toegewezen. In Europa worden internetprotocoladressen op geografische basis aan de lidstaten toegewezen. De uitwisseling van gegevens tussen de lidstaten in het kader van Besluit 2008/615/JBZ vindt plaats over een Europees logisch gesloten IP-netwerk.

Testomgeving

Om een goed werkende omgeving voor dagelijks operationeel gebruik tussen de verbonden lidstaten tot stand te kunnen brengen, moet in het gesloten netwerk een testomgeving worden gecreëerd voor nieuwe lidstaten die zich wensen aan te sluiten. Daartoe is een reeks parameters gespecificeerd, zoals IP-adressen, netwerksettings, e-maildomeinen en accounts voor gebruikers van de applicatie, die op de site van de betreffende lidstaat moeten worden gecreëerd. Verder is er een reeks pseudo-DNA-profielen aangemaakt die voor de tests zullen worden gebruikt.

5.7.5. Configuratieparameters

Er wordt een beveiligd e-mailsysteem ingesteld, dat het domein eu-admin.net gebruikt. Dit domein en de bijbehorende adressen zijn niet toegankelijk vanuit een locatie die zich niet op het Europese TESTA-domein bevindt, omdat de namen alleen op de centrale DNS-server van TESTA worden herkend en deze server van het internet is afgeschermd.

De DNS-dienst van TESTA zorgt voor de mapping van deze adressen van de TESTA-site („host"-namen) en de corresponderende IP-adressen. Voor elk lokaal domein wordt aan de centrale DNS-server van TESTA een e-mailtoegang toegevoegd, zodat alle e-mailberichten die naar lokale TESTA-domeinen worden verzonden, naar de centrale e-mailrelay van TESTA worden doorgestuurd. Vanuit deze centrale e-mailrelay van TESTA worden de berichten vervolgens naar de specifieke e-mailserver van het lokale domein doorgestuurd; daarvoor worden de e-mailadressen van het lokale domein gebruikt. Door e-mailberichten op deze manier door te sturen, passeert gevoelige informatie in e-mailberichten alleen door de Europese gesloten netwerkinfrastructuur, en niet over het onveilige internet.

Op de sites van alle lidstaten moeten subdomeinen (***bold italics***) worden gecreëerd die er als volgt uitzien:

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

„Member State-code" staat voor een van de uit twee letters bestaande lidstaatcodes (bv. AT, BE, enz.);

„***application-type***" een van de volgende waarden is: DNA of FP (vingerafdruk).

Toepassing van het bovenstaande levert de volgende subdomeinen op voor de lidstaten:

Lidstaat	Subdomeinen	Commentaar
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	

Lidstaat	Subdomeinen	Commentaar
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	

Lidstaat	Subdomeinen	Commentaar
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	

HOOFDSTUK 2: **Uitwisseling van dactyloscopische gegevens (interfacecontroledocument)**

In het navolgende interfacecontroledocument wordt omschreven aan welke eisen de uitwisseling van dactyloscopische gegevens tussen de geautomatiseerde vingerafdrukidentificatiesystemen (AFIS — Automated Fingerprint Identification Systems) van de lidstaten moet voldoen. Een en ander is gebaseerd op de implementatie van ANSI/NIST-ITL 1-2000 (INT-I, versie 4.22b) in het kader van Interpol.

Deze versie bevat de basisdefinities voor de logische records van type 1, type 2, type 4, type 9, type 13 en type 15, die nodig zijn voor het verwerken van dactyloscopische gegevens (beelden en minutiae).

1. ***Overzicht van de bestandsinhoud***

Een bestand met dactyloscopische gegevens bestaat uit verschillende logische records. In de oorspronkelijke norm ANSI/NIST-ITL 1-2000 worden 16 recordsoorten gespecificeerd. De records, en de velden en subvelden in de records, worden van elkaar gescheiden door middel van ASCII-tekens.

Voor de uitwisseling van informatie tussen de verzendende dienst en de dienst van bestemming worden slechts 6 recordtypes gebruikt:

Type 1 → informatie over de te verrichten opdracht
Type 2 → alfanumerieke gegevens over de persoon/zaak
Type 4 → dactyloscopische grijswaardenbeelden in hoge resolutie
Type 9 → minutiae record
Type 13 → sporenbeeld in variabele resolutie
Type 15 → handpalmafdrukbeeld in variabele resolutie

1.1. *Type 1 — Bestandsaanhef*

Deze record bevat informatie over de routing en een beschrijving van de structuur van de rest van het bestand. Dit recordtype bevat tevens een omschrijving van de soorten opdrachten, die in de volgende algemene categorieën kunnen worden onderverdeeld:

1.2. *Type 2 — Beschrijvende tekst*

Deze record bevat tekstinformatie die van belang is voor de verzendende en voor de ontvangende dienst.

1.3. *Type 4 — Grijswaardenbeeld in hoge resolutie*

Deze record wordt gebruikt voor de uitwisseling van dactyloscopische grijswaardenbeelden in hoge resolutie (8 bits), gesampled tegen 500 pixels per inch. De dactyloscopische beelden moeten worden gecomprimeerd met behulp van een WSQ-algoritme in een maximale van 15:1. Andere comprimeringsalgoritmen of niet-gecomprimeerde beelden mogen niet worden gebruikt.

1.4. *Type 9 — Minutiae record*

Type 9-records worden gebruikt om lijnkenmerken of minutiaegegevens uit te wisselen. Dit soort records is bedoeld om enerzijds overbodige herhalingen van AFIS-coderingen te voorkomen, en anderzijds de transmissie van AFIS-codes met minder gegevens dan de corresponderende beelden mogelijk te maken.

1.5. *Type 13 — Sporenbeeld in variabele resolutie*

Deze record wordt gebruikt om beelden (in variabele resolutie) van vinger- en handpalmafdruksporen uit te wisselen, tezamen met alfanumerieke informatie over de textuur. De scanresolutie van de beelden bedraagt 500 pixels per inch, met 256 grijsniveaus. Indien het beeld van de sporen van voldoende kwaliteit is, wordt het door middel van een WSQ-algoritme gecomprimeerd. Indien nodig kan bilateraal worden afgesproken de beeldresolutie te verscherpen tot meer dan 500 pixels per inch en meer dan 256 grijsniveaus. In dat geval verdient het sterke aanbeveling gebruik te maken van JPEG 2000 (zie aanhangsel 7).

1.6. *Handpalmafdrukbeeld in variabele resolutie*

Voor het uitwisselen van handpalmafdrukbeelden in variabele resolutie met alfanumerieke informatie over de textuur worden tagged-field beeldrecords van type 15 gebruikt. De scanresolutie van de beelden bedraagt 500 pixels per inch, met 256 grijsniveaus. Om het gegevensvolume te beperken, worden alle handpalmafdrukbeelden door middel van een WSQ-algoritme gecomprimeerd. Indien nodig kan bilateraal worden afgesproken de beeldresolutie te verscherpen tot meer dan 500 pixels per inch en meer dan 256 grijsniveaus. In dat geval verdient het sterke aanbeveling gebruik te maken van JPEG 2000 (zie aanhangsel 7).

2. ***Recordformaat***

Een opdrachtbestand bestaat uit één of meer logische records. Voor elke logische record in het bestand moeten, afhankelijk van het recordtype, verschillende informatievelden bestaan. Elk informatieveld kan één of meer basale informatie-elementen bevatten die elk uit één waarde bestaan. Samen worden deze elementen gebruikt om de verschillende aspecten van de gegevens van dat veld kenbaar te maken. Een informatieveld kan ook bestaan uit één of meer informatie-elementen die worden gegroepeerd en in een veld verschillende keren worden herhaald. Een dergelijke groep informatie-elementen wordt subveld genoemd. Een informatieveld kan dus uit één of meer subvelden met informatie-elementen bestaan.

2.1. *Informatiescheidingstekens*

In tagged field logische records worden vier ASCII-infomatiescheidingstekens gebruikt om informatie af te bakenen. Afgebakende informatie kan zijn: elementen in een veld of subveld, velden in een logische record, of herhalingen van subvelden. Deze informatiescheidingstekens worden gedefinieerd volgens de norm ANSI X3.4. Deze karakters worden gebruikt om informatie in logische zin te scheiden en te kwalificeren. De hiërarchische verhouding is als volgt: het bestandscheidingsteken „FS" (File Separator) is het meest inclusieve teken, gevolgd door het groepsscheidingsteken „GS" (Group Separator), het recordscheidingsteken „RS" (Record Separator) en, ten slotte, het eenheidscheidingsteken „Verenigde Staten" (Unit Separator). Tabel 1 bevat een lijst van deze ASCII-scheidingstekens, met een beschrijving van het doel waarvoor zij in deze norm worden gebruikt.

Vanuit functioneel oogpunt moeten informatiescheidingstekens worden gezien als indicatie van het soort gegevens dat volgt. Het teken „Verenigde Staten" scheidt individuele informatie-elementen binnen een veld of subveld. Dit duidt erop dat de informatie die volgt, een stukje data voor dat veld of subveld is. Wanneer verschillende subvelden binnen een veld door het teken „RS" worden gescheiden, duidt dit op het begin van de volgende groep herhaalde informatie-elementen. Het scheidingsteken „GS" tussen informatievelden duidt op het begin van een nieuw veld voorafgaand aan het veldidentificatienummer dat moet verschijnen. Het begin van een nieuwe logische record moet worden aangegeven door het teken „FS".

De vier tekens hebben slechts een betekenis wanneer ze als datascheidingstekens in de velden van ASCII-tekstrecords worden gebruikt. Wanneer ze in binaire beeldrecords of in binaire velden worden gebruikt, hebben ze geen specifieke betekenis — ze maken louter deel uit van de uitgewisselde gegevens.

Normaliter komen er geen lege velden of informatie-elementen voor; bijgevolg mag er slechts één scheidingsteken staan tussen twee gegevenselementen. Er is een uitzondering op deze regel, namelijk wanneer de gegevens in velden dan wel informatie-elementen in een opdracht niet beschikbaar zijn, ontbreken of facultatief zijn en de verwerking van de opdracht niet afhankelijk is van die specifieke gegevens. Wanneer er in zulke gevallen verschillende scheidingstekens op elkaar volgen, moeten deze samen verschijnen en hoeven er geen „nepgegevens" te worden tussengevoegd.

Voor de definitie van een veld dat uit drie informatie-elementen bestaat, geldt het volgende: indien de informatie voor het tweede informatie-element ontbreekt, komen tussen het eerste en het derde informatie-element twee aanliggende „Verenigde Staten"-informatiescheidingstekens voor. Indien zowel het tweede als het derde informatie-element zou ontbreken, zouden drie scheidingstekens moeten worden gebruikt — twee „Verenigde Staten"-tekens plus het scheidingsteken voor het veld- of subveldeinde. De algemene regel is dat indien een of meer verplichte of facultatieve informatie-elementen niet beschikbaar zijn voor een veld of subveld, het overeenkomstige aantal scheidingstekens wordt tussengevoegd.

Het is mogelijk dat combinaties van twee of meer van de vier beschikbare scheidingstekens naast elkaar voorkomen. Indien gegevens ontbreken of niet beschikbaar zijn voor informatie-elementen, subvelden of velden, moet er één scheidingsteken minder voorkomen dan het vereiste aantal gegevenselementen, subvelden of velden.

Tabel 1: gebruikte scheidingstekens

Code	Type	Description	Hexadecimal Value	Decimal Value
Verenigde Staten	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. *Recordindeling*

In het geval van tagged-field logische records wordt elk gebruikt informatieveld volgens deze norm genummerd. Het formaat van elk veld bestaat uit het nummer van het type logische record, gevolgd door een punt „.", een veldnummer gevolgd door een dubbele punt „:", en vervolgens de informatie die bij dat veld hoort. Het tagged-field nummer kan om het even welk getal van één tot negen cijfers zijn tussen de punt „." en de dubbele punt „:". Het wordt geïnterpreteerd als veldnummer dat een positief geheel getal is. Dit impliceert dat een veldnummer met de waarde „2.123:" gelijk is aan en op dezelfde manier moet worden geïnterpreteerd als een veldnummer met de waarde „2.000000123:".

In dit document wordt bij wijze van voorbeeld een getal van drie cijfers gebruikt voor het opsommen van de velden in elk van de in het document beschreven tagged-field logische records. Veldnummers nemen de volgende vorm aan: „TT.xxx:", waarbij de „TT" staat voor het recordtype, bestaande uit één of twee karakters, gevolgd door een punt. De volgende drie karakters bevatten het desbetreffende veldnummer, gevolgd door een dubbele punt. De dubbele punt wordt gevolgd door beschrijvende ASCII-informatie of door de beeldgegevens.

Logische records van type 1 en type 2 bevatten uitsluitend ASCII-tekstgegevensvelden. De volledige lengte van de record (met inbegrip van de veldnummers, dubbele punten en scheidingstekens) wordt als eerste ASCII-veld vastgelegd in elk van deze recordtypes. Het controleteken van het ASCII-bestandscheidingsteken „FS" (dat het einde van de logische record of opdracht aangeeft) volgt de laatste byte van de ASCII-informatie en wordt meegerekend in de lengte van de record.

Anders dan in het geval van tagged-field records bevat de type 4-record uitsluitend binaire gegevens die worden vastgelegd als geordende binaire velden met een vaste lengte. De volledige lengte van de record wordt vastgelegd in het eerste binaire veld van vier bytes van elke record. Voor deze binaire record worden geen recordnummer met punt en geen veldidentificatienummer met daarop volgende dubbele punt vastgelegd. Aangezien alle veldlengtes van deze record ofwel vast ofwel gespecificeerd zijn, wordt geen enkele van de vier scheidingstekens („Verenigde Staten", „RS", „GS" of „FS") anders geïnterpreteerd dan als binair gegeven. Voor binaire records wordt het „FS"-teken niet als bestandscheidingsteken of als opdrachteindeteken gebruikt.

3. ***Logische-recordtype 1: bestandsaanhef***

Deze record beschrijft de structuur van het bestand, het soort bestand en andere belangrijke informatie. De voor type 1-velden gebruikte karakterreeks bevat uitsluitend de 7-bits ANSI-code voor onderlinge uitwisseling van informatie.

3.1. *Velden voor logische-recordtype 1*

3.1.1. Veld 1.001: logische-recordlengte (Logical Record Length — LEN)

Dit veld bevat het totale aantal bytes in de volledige logische-recordtype 1. Het veld begint met „1.001:", gevolgd door de totale lengte van de record, dit wil zeggen elk karakter van elk veld, plus de informatiescheidingstekens.

3.1.2. Veld 1.002: versienummer (Version Number — VER)

Om ervoor te zorgen dat de gebruikers weten welke versie van de ANSI/NIST-norm wordt gebruikt, specificeert dit veld van 4 bytes het versienummer van de norm die wordt geïmplementeerd door de software of het systeem waarmee het bestand is gecreëerd. De eerste twee bytes specificeren het belangrijkste referentienummer van de gebruikte versie, de tweede twee het minder belangrijke nummer van herziening. De originele norm van 1986 zou bijvoorbeeld als eerste versie worden beschouwd en met „0100" worden aangegeven, terwijl de huidige ANSI/NIST-ITL 1-2000-norm „0300" is.

3.1.3. Veld 1.003: bestandsinhoud (File Content — CNT)

Dit veld bevat een opsomming van alle records in het bestand, per recordtype en in de volgorde waarin de records in het logisch bestand voorkomen. Het bestaat uit één of meer subvelden, die elk twee informatie-elementen bevatten die één logische record uit het desbetreffende bestand beschrijven. De subvelden worden in dezelfde volgorde opgenomen als die waarin de records worden geregistreerd en verzonden.

Het eerste informatie-element in het eerste subveld is „1", hetgeen verwijst naar dit type 1-record. Het wordt gevolgd door een tweede informatie-element dat het aantal andere records in het bestand bevat. Dit aantal is ook gelijk aan het totaal van de overige subvelden van veld 1.003.

De overige subvelden worden elk aan één record in het bestand gekoppeld, en de sequentie van de subvelden komt met die van de records overeen. Elk subveld bevat twee informatie-elementen. Het eerste is een identificatie van het type record. Het tweede is de IDC van de record. Het karakter „Verenigde Staten" wordt gebruikt om de twee informatie-elementen van elkaar te scheiden.

3.1.4. Veld 1.004: Soort opdracht (Type of Transaction — TOT)

Dit veld bevat een uit drie letters bestaand „ezelsbruggetje" ter aanduiding van het soort opdracht. Deze codes kunnen verschillen van de codes die in andere implementaties van de ANSI/NIST-norm worden gebruikt.

CPS: Criminal Print-to-Print Search (afdrukbevraging in een afdrukkendatabank voor strafrechtelijke doeleinden). Het gaat hierbij om een verzoek tot bevraging van een afdrukkendatabank met betrekking tot een record die verband houdt met een strafbaar feit. De afdrukken van de betrokkene moeten als WSQ-gecomprimeerde beelden in het bestand worden opgenomen.

In het geval van een „No-HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record.

In het geval van een „HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record,

— 1 tot 14 type-4 record(s).

In tabel A.6.1 (aanhangsel 6) wordt schematisch weergegeven wat de opdracht „CPS" inhoudt.

PMS: Print-to-Latent Search (afdrukbevraging in een sporendatabank). Deze opdracht wordt gegeven om voor een reeks afdrukken een bevraging te verrichten in een databank van niet-geïdentificeerde sporen. Het antwoord bevat een Hit/No-Hit-melding van het AFIS waarin de bevraging is verricht. Indien er verschillende niet-geïdentificeerde sporen zijn, worden er verschillende SRE's teruggestuurd met telkens één spoor per opdracht. De afdrukken van de betrokkene moeten als WSQ-gecomprimeerde beelden in het bestand worden opgenomen.

In het geval van een „No-HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record.

In het geval van een „HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record,

— 1 type-13 record.

In tabel A.6.1 (aanhangsel 6) wordt schematisch weergegeven wat de opdracht „PMS" inhoudt.

MPS: Latent-to-Print Search (sporenbevraging in een afdrukkendatabank). Deze opdracht wordt gegeven wanneer voor een bepaald spoor een bevraging moet worden verricht in een afdrukkendatabank. De informatie over de minutiae van het spoor moet samen met het beeld (met WSQ-comprimering) in het bestand worden opgenomen.

In het geval van een „No-HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record.

In het geval van een „HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record,

— 1 type-4 of type-15 record.

In tabel A.6.4 (aanhangsel 6) wordt schematisch weergegeven wat de opdracht „MPS" inhoudt.

MMS: Latent-to-Latent Search (sporenbevraging in een sporendatabank). In dit geval bevat het bestand een spoor waarvoor een bevraging moet worden verricht in een databank van niet-geïdentificeerde sporen met de bedoeling verbanden te leggen tussen verschillende plaatsen delict. De informatie over de minutiae van het spoor moet samen met het beeld (met WSQ-comprimering) in het bestand worden opgenomen.

In het geval van een „No-HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record.

In het geval van een „HIT" worden de volgende logische records teruggestuurd:

— 1 type-1 record,

— 1 type-2 record,

— 1 type-13 record.

In tabel A.6.4 (aanhangsel 6) wordt schematisch weergegeven wat de opdracht „MMS" inhoudt.

SRE: deze opdracht wordt door de dienst van bestemming teruggestuurd als antwoord op toegezonden dactyloscopische gegevens. Het antwoord bevat een Hit/No-Hit-melding van het AFIS waarin de bevraging is verricht. Indien er verschillende mogelijke „hits" zijn, worden er verschillende SRE's teruggestuurd met telkens één mogelijke „hit".

In tabel A.6.2 (aanhangsel 6) wordt schematisch weergegeven wat de opdracht „SRE" inhoudt.

ERR: foutmelding die wordt teruggestuurd door het AFIS van bestemming. Een ERR bevat een berichtveld (ERM) waarin de vastgestelde fout wordt aangegeven. De volgende logische records worden teruggestuurd:

— 1 type-1 record,

— 1 type-2 record.

In tabel A.6.3 (aanhangsel 6) wordt schematisch aangegeven wat de opdracht „ERR" inhoudt.

Tabel 2: Toegestane codes in opdrachten

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	—	—	—	—

Verklaring:

M = Mandatory (verplicht)
M* = het is mogelijk dat slechts één van de beide recordtypes is opgenomen
O = Optional (facultatief)
C = Conditional — is afhankelijk van de beschikbaarheid van gegevens
— = niet toegestaan
1* = Conditional — is afhankelijk van de ouderdom van de systemen

3.1.5. Veld 1.005: opdrachtdatum (Date of Transaction — DAT)

Dit veld bevat de datum waarop de opdracht is gegeven en moet beantwoorden aan de volgende ISO-standaardnotering: YYYYMMDD

waarbij YYYY het jaar is, MM de maand en DD de dag. Getallen uit één cijfer worden in de notering door een nul voorafgegaan. Bijvoorbeeld: „19931004" staat voor 4 oktober 1993.

3.1.6. Veld 1.006: prioriteit (Priority — PRY)

In dit facultatieve veld wordt de prioriteit van het verzoek, gaande van 1 tot 9, bepaald. „1" is de hoogste prioriteit; „9" de laagste. Opdrachten met prioriteit „1" moeten onmiddellijk worden verwerkt.

3.1.7. Veld 1.007: identificatie dienst van bestemming (Destination Agency Identifier — DAI)

In dit veld wordt gespecificeerd voor welke dienst de opdracht bestemd is.

Het bestaat uit twee informatie-elementen van het volgende formaat: CC/dienst.

Het eerste informatie-element is de ISO 3166-landencode (twee alfanumerieke karakters). Het tweede element, de dienst, is een identificatie van de dienst in vrije tekst van maximaal 32 alfanumerieke karakters.

3.1.8. Veld 1.008: identificatie dienst van herkomst (Originating Agency Identifier — ORI)

In dit veld wordt de originator van het bestand gespecificeerd; het heeft hetzelfde formaat als de DAI (veld 1.007).

3.1.9. Veld 1.009: opdrachtcontrolenummer (Transaction Control Number — TCN)

Dit is een controlenummer dat voor referentiedoeleinden wordt gebruikt. Dit nummer moet door de computer worden gegenereerd en dient het volgende formaat te hebben: YYSSSSSSSSA

waarbij YY het jaar van de opdracht is, SSSSSSSS een serienummer van acht cijfers en A een controleteken dat wordt gegenereerd door de procedure van aanhangsel 2 te volgen.

Indien er geen TCN beschikbaar is, wordt het veld YYSSSSSSSS met nullen gevuld en wordt een controleteken gegenereerd zoals hierboven is beschreven.

3.1.10. Veld 1.010: antwoord opdrachtcontrole (Transaction Control Response — TCR)

Wanneer een verzoek is verzonden waarop dit het antwoord is, bevat dit facultatieve veld het opdrachtcontrole-nummer van het verzoekbericht. Het heeft daarom hetzelfde formaat als het TCN (veld 1.009).

3.1.11. Veld 1.011: native scanning-resolutie (NSR)

Dit veld specificeert de normale scanresolutie van het systeem dat door de originator van het bericht wordt ondersteund. De resolutie wordt gespecificeerd als twee cijfers, gevolgd door een decimaal punt en nogmaals twee cijfers.

Voor alle opdrachten in verband met Besluit 2008/615/JBZ bedraagt de bemonsteringsverhouding 500 pixels/inch of 19,68 pixels/mm.

3.1.12. Veld 1.012: nominale transmissieresolutie (Nominal Transmitting Resolution — NTR)

In dit veld van 5 bytes wordt de nominale transmissieresolutie van de doorgezonden beelden gespecificeerd. De resolutie wordt aangegeven in pixels/mm, in hetzelfde formaat als NSR (veld 1.011).

3.1.13. Veld 1.013: domeinnaam (DOM)

Dit verplichte veld bevat de identificatie van de domeinnaam ten behoeve van de implementatie van de gebruikergebonden type 2-logische record. Het bestaat uit de volgende twee informatie-elementen: „INT-I {Verenigde Staten}4.22{GS}".

3.1.14. Veld 1.014: Greenwich mean time (GMT)

Dit verplichte veld bevat de datum en tijd in universele Greenwich Mean Time (GMT)-weergave. Het GMT-veld dat wordt gebruikt bevat de universele datum en de lokale datum van veld 1.005 (DAT). Door het GMT-veld te gebruiken, worden inconsistenties in verband met lokale tijdsaanduidingen geëlimineerd die ontstaan wanneer een bericht en het antwoord daarop worden verzonden tussen twee plaatsen die in verschillende tijdszones liggen. GMT geeft een universele datum en een 24-urenkloktijd die onafhankelijk is van tijdszones. Dit veld wordt weergegeven als „CCYYMMDDHHMMSSZ", een reeks van 15 karakters die een opeenvolging zijn van de datum en de GMT en eindigt met een „Z". De karakters „CCYY" staan voor het jaar van het bericht, de karakters „MM" staan voor de maand (in tientallen en eenheden), de karakters „DD" staan voor de dag (in tientallen en eenheden), de karakters „HH" geven het uur weer, de „MM" de minuten en de „SS" de seconden. De volledige datum mag niet later zijn dan de actuele datum.

4. ***Logische-recordtype 2: beschrijving***

De structuur van deze record is voor een groot deel niet volgens de originele ANSI/NIST-norm gedefinieerd. De record bevat informatie die van specifiek belang is voor de diensten die het bestand verzenden of ontvangen. Om ervoor te zorgen dat met elkaar communicerende dactyloscopiesystemen verenigbaar zijn, mag de record alleen de hieronder opgesomde velden bevatten. Dit document specificeert welke velden verplicht zijn en welke facultatief, en bevat tevens een definitie van de structuur van de individuele velden.

4.1. *Velden voor logische-recordtype 2*

4.1.1. Veld 2.001: logische-recordlengte (Logical Record Length — LEN)

Dit verplichte veld bevat de lengte van deze type 2-record en specificeert het totale aantal bytes, daaronder begrepen elk karakter van elk veld in de record, plus de informatiescheidingstekens.

4.1.2. Veld 2.002: beeldkarakterisering (Image Designation Character — IDC)

De IDC in dit verplichte veld is een ASCII-weergave van de IDC zoals gedefinieerd in het bestandsinhoudveld (CNT) van de type 1-record (veld 1.003).

4.1.3. Veld 2.003: systeeminformatie (SYS)

Met dit verplichte veld van 4 bytes wordt aangegeven aan welke versie van de INT-I de desbetreffende type 2-record voldoet.

De eerste twee bytes specificeren het belangrijkste versienummer, de volgende twee het minder belangrijke nummer van herziening. Deze implementatie is bijvoorbeeld gebaseerd op INT-I versie 4, 22e herziening, en zou als volgt worden weergegeven: „0422".

4.1.4. Veld 2.007: zaaknummer (Case Number — CNO)

Dit is een nummer dat door het lokale dactyloscopiebureau wordt gegeven aan een verzameling mogelijke sporen die op een plaats delict zijn gevonden. Het formaat ziet er als volgt uit: CC/nummer

waarbij CC de uit twee alfanumerieke karakters bestaande Interpol-landencode is, en het nummer volgens de lokale richtsnoeren wordt weergegeven met ten hoogte 32 alfanumerieke karakters.

Door middel van dit veld kan het systeem mogelijke sporen van een bepaald delict identificeren.

4.1.5. Veld 2.008: sequentienummer (SQN)

In dit veld wordt elke sequentie van mogelijke sporen in een zaak gespecificeerd. Het veld is maximaal 4 numerieke karakters lang. Een sequentie is een spoor of reeks sporen die worden gegroepeerd, zodat deze kunnen worden geregistreerd en/of bevraagd. Deze definitie houdt in dat zelfs individuele sporen altijd een sequentienummer moeten krijgen.

Dit veld kan samen met de MID (veld 2.009) worden opgenomen om een bepaald spoor in een sequentie te identificeren.

4.1.6. Veld 2.009: spooridentificatie (Latent Identifier — MID)

Dit is een specificatie van een individueel spoor in een sequentie. De waarde is één enkele letter of twee letters, waarbij „A" voor het eerste spoor staat, „B" voor het tweede, en zo verder tot een limiet van „ZZ". Dit veld wordt analoog aan het sporensequentienummer bedoeld in de beschrijving voor het sequentienummer (veld 2.008) gebruikt.

4.1.7. Veld 2.010: strafrechtelijk referentienummer (Criminal Reference Number — CRN)

Dit is een uniek referentienummer dat door een nationale instantie aan iemand wordt toegekend wanneer deze voor het eerst van een strafbaar feit wordt beschuldigd. Niemand kan meer dan één CRN of hetzelfde CRN als een andere persoon hebben in hetzelfde land. Eenzelfde persoon kan wel verscheidene strafrechtelijke referentienummers hebben in verschillende landen; deze kunnen door de landencode van elkaar worden onderscheiden.

Het formaat van het CRN-veld ziet er als volgt uit: CC/nummer

waarbij CC de uit 2 alfanumerieke karakters bestaande ISO 3166-code is, en het nummer volgens de nationale richtlijnen van de verzendende instantie wordt weergegeven met maximaal 32 alfanumerieke karakters.

Voor opdrachten in verband met Besluit 2008/615/JBZ wordt dit veld gebruikt voor het nationale strafrechtelijke referentienummer van de verzendende instantie, dat gekoppeld is aan de beelden in type 4- of type 15-records.

4.1.8. Veld 2.012: identificatienummer (Miscellaneous Identification Number — MN1)

Dit veld bevat het CRN (veld 2.010) dat in het kader van een CPS- of PMS-opdracht is verzonden, zonder de inleidende landencode.

4.1.9. Veld 2.013: identificatienummer (Miscellaneous Identification Number — MN2)

Dit veld bevat het CNO (veld 2.007) dat in het kader van een MPS- of MMS-opdracht is verzonden, zonder de inleidende landencode.

4.1.10. Veld 2.014: identificatienummer (Miscellaneous Identification Number — MN3)

Dit veld bevat het SQN (veld 2.008) dat in het kader van een MPS- of MMS-opdracht is verzonden.

4.1.11. Veld 2.015: identificatienummer (Miscellaneous Identification Number — MN4)

Dit veld bevat de MID (veld 2.009) die in het kader van een MPS- of MMS-opdracht is verzonden.

4.1.12. Veld 2.063: aanvullende informatie (INF)

In het geval van een SRE-opdracht naar aanleiding van een PMS-verzoek wordt in dit veld informatie verstrekt over de vinger die aanleiding heeft gegeven tot een mogelijke „HIT". Het formaat van het veld ziet er als volgt uit:

NN waarbij NN de vingerpositiecode is, als gedefinieerd in tabel 5 (twee cijfers).

In alle andere gevallen is het veld facultatief. Het bestaat uit maximaal 32 alfanumerieke karakters en kan aanvullende informatie verschaffen over het verzoek.

4.1.13. Veld 2.064: respondentenlijst (Respondents List — RLS)

Dit veld bevat ten minste twee subvelden. In het eerste subveld wordt beschreven welke bevraging is verricht, door middel van het uit drie letters bestaande „ezelsbruggetje" waarmee in veld 1.004 (TOT) de soort opdracht wordt gespecificeerd. Het tweede subveld bevat één karakter. Een „I" wordt gebruikt om een HIT aan te geven en een „N" wordt gebruikt om aan te geven dat er geen overeenkomsten zijn (NOHIT). In een derde subveld worden de sequentie-identificator voor de aangetroffen mogelijke hit en het totale aantal mogelijke hits opgenomen, gescheiden door een schuine streep. Indien er verschillende mogelijke hits zijn, worden verschillende berichten teruggestuurd.

In het geval van een mogelijke HIT wordt in een vierde subveld de score weergegeven, die maximaal tien cijfers lang is. Indien de HIT is bevestigd, wordt de waarde van dit subveld omschreven als „999999".

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

Indien het externe AFIS geen scores toekent, moet op het daarvoor bestemde punt een score „nul" worden gebruikt.

4.1.14. Veld 2.074: status/foutmelding (Status/Error Message Field — ERM)

Dit veld bevat foutmeldingen naar aanleiding van opdrachten, die naar de indiener van het verzoek worden teruggestuurd als onderdeel van een foutbericht.

Tabel 3: Foutmeldingen

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

Foutmeldingen met een waarde tussen 100 en 199:

Deze foutmeldingen houden verband met de validering van de ANSI/NIST-records en worden gedefinieerd als volgt:

<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>...

waarbij:

— de code „error_code" uitsluitend aan een specifieke reden is gerelateerd (zie tabel 3);

— „field_id" het ANSI/NIST-veldnummer van het incorrecte veld is (bv. 1.001, 2.001 ...) in het volgende formaat: <record_type>.field_id>.sub_field_id>

— de dynamische tekst een meer gedetailleerde dynamische beschrijving van de fout bevat;

— LF een line feed is waarmee fouten van elkaar worden gescheiden indien er zich meer dan één fout heeft voorgedaan;

— voor type 1-records het ICD wordt gedefinieerd als „-1".

Voorbeeld:

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

Dit veld is verplicht voor foutberichten.

4.1.15. Veld 2.320: geraamd aantal mogelijke hits (Expected Number of Candidates — ENC)

Dit veld bevat het door de verzoekende dienst geraamde maximale aantal mogelijke hits voor verificatie. De waarde van het ENC mag niet groter zijn dan de in tabel 11 vastgelegde waarden.

5. ***Logische-recordtype 4: grijswaardenbeeld in hoge resolutie***

Type 4-records zijn binaire records (geen ASCII). Dit betekent dat elk veld een specifieke plaats in de record inneemt en dat alle velden bijgevolg verplicht zijn.

De norm maakt het mogelijk om in een en dezelfde record zowel de beeldgrootte als de beeldresolutie te specificeren. Daartoe moeten logische records van type 4 dactyloscopische beelden bevatten die met een nominale pixeldensiteit van 500 tot 520 pixels per inch worden doorgestuurd. Voor nieuwe vormen gaat de voorkeur uit naar een pixeldensiteit van 500 pixels per inch, of 19,68 pixels per mm. De door de INT-I gespecificeerde densiteit bedraagt 500 pixels per inch, met dien verstande dat vergelijkbare systemen zonder vaste voorkeursdensiteit met elkaar kunnen communiceren, zolang het aantal pixels per inch maar 500 à 520 bedraagt.

5.1. *Velden voor logische-recordtype 4*

5.1.1. Veld 4.001: logische-recordlengte (Logical Record Length — LEN)

Dit veld van 4 bytes bevat de lengte van deze type 4-record en specificeert het totale aantal bytes, daaronder begrepen elke byte van elk veld in de record.

5.1.2. Veld 4.002: beeldkarakterisering (Image Designation Character — IDC)

Dit is een binaire weergave (1 byte) van het IDC-nummer in de bestandsaanhef.

5.1.3. Veld 4.003: afdruktype (IMP)

Het afdruktype is een veld van 1 byte op de zesde bytepositie in de record.

Tabel 4: Vingerafdruktype

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. Veld 4.004: vingerpositie (Finger Position — FGP)

Dit veld heeft een vaste lengte van 6 bytes en bekleedt de zevende tot en met de twaalfde bytepositie van een type 4-record. Het bevat mogelijke vingerposities, beginnend vanaf de meest linkse byte (zevende positie in de record). De bekende of meest waarschijnlijke vingerpositie is gebaseerd op tabel 5. In totaal kan nog voor vijf andere vingers een referentie worden opgenomen; hiertoe worden, in hetzelfde formaat, de vingerposities beurtelings in de resterende 5 bytes ingevoerd. Indien minder dan vijf vingerpositiewaarden worden gebruikt, worden de niet gebruikte bytes opgevuld met een binair 255-karakter. Bij de waardebepaling van vingerposities wordt code 0 gebruikt voor „onbekend".

Tabel 5: Vingerpositiecode en maximale afmetingen

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

Voor sporen die op de plaats delict zijn aangetroffen, worden alleen de codes 0 tot 10 gebruikt.

5.1.5. Veld 4.005: beeldscanresolutie (Image Scanning Resolution — ISR)

Dit veld van 1 byte neemt de 13e bytepositie in een type-4 record in. Als de waarde ervan „0" is, betekent dit dat het beeld is gesampled met de aanbevolen scanverhouding van 19,68 pixels/mm (500 pixels per inch). Als de waarde „1" is, betekent dit dat het beeld is gesampled met een andere scanverhouding, die in de type-1 record wordt gespecificeerd.

5.1.6. Veld 4.006: lengte horizontale lijn (Horizontal Line Length — HLL)

Dit veld bekleedt de 14e en 15e bytepositie in een type-4 record. Het geeft het aantal pixels in elke scanlijn weer. De eerste byte is de belangrijkste.

5.1.7. Veld 4.007: lengte verticale lijn (Vertical Line Length — VLL)

In dit veld, op de 16e en de 17e bytepositie, wordt het aantal scanlijnen van het beeld vastgelegd. De eerste byte is de belangrijkste.

5.1.8. Veld 4.008: comprimeringsalgoritme van de grijswaarden (Gray-scale Compression Algorithm — GCA)

In dit veld van 1 byte wordt de algoritme voor de comprimering van de grijswaarden gespecificeerd die voor het coderen van de beeldgegevens wordt gebruikt. In dit geval betekent een binaire code 1 dat een WSQ-comprimering is gebruikt (aanhangsel 7).

5.1.9. Veld 4.009: beeld

Dit veld bevat een bytestream die het beeld weergeeft. Het ligt voor de hand dat de structuur van dit veld afhangt van de gebruikte comprimeringsalgoritme.

6. ***Logische-recordtype 9: minutiaerecord***

Type-9 records bevatten een beschrijving, in ASCII-tekst, van de minutiae en aanverwante (gecodeerde) informatie van sporen. In het geval van bevragingen van sporen zijn er geen beperkingen wat het aantal type-9 records in een bestand betreft; per view of spoor is er een aparte record.

6.1. *Minutiae-extractie*

6.1.1. Identificatie van het soort minutiae

In deze norm worden drie identificatiecijfers vastgelegd waarmee het soort minutiae wordt beschreven. Een overzicht staat in tabel 6. Een eindigende lijn wordt aangegeven als type 1. Een bifurcatie (vertakking) wordt aangegeven als type 2. Indien minutiae niet duidelijk als een van de twee bovengenoemde soorten kunnen worden gecategoriseerd, worden deze als type 0, ofwel „andere", aangegeven.

Tabel 6: soorten minutiae

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Plaatsing en soort minutiae

Om de plaatsing (locatie en hoekrichting) van individuele minutiae te bepalen wordt de volgende methode — die een uitbreiding is van de huidige norm INCITS 378-2004 — toegepast, zodat de templates stroken met deel 5 van norm ANSI INCITS 378-2004.

De positie of locatie van een minutia die een eindigende lijn voorstelt, is het vertakkingspunt van het mediale skelet in de „voren" direct voor de eindigende lijn. Bij verdunning van de drie benen van de „voren" tot een 1 pixel breed skelet, bepaalt het snijpunt de locatie van de minutia. Naar analogie is de locatie van de minutia in het geval van een bifurcatie het vertakkingspunt van het mediale skelet van de lijn. Bij verdunning van de drie benen van de lijn tot een 1 pixel breed skelet, bepaalt het snijpunt van de drie benen de locatie van de minutia.

Na omzetting van de eindigende lijnen in bifurcaties worden de minutiae van het dactyloscopisch beeld als bifurcaties weergegeven. De X- en Y-pixelassen van het snijpunt van de drie benen van elke minutia kunnen direct worden getrokken. De richting van de minutia kan worden bepaald aan de hand van elke skeletvormige bifurcatie. De drie benen van elke skeletvormige bifurcatie moeten worden beschouwd en het eindpunt van elk been moet worden bepaald. Figuur 6.1.2 illustreert de drie methodes die worden gebruikt om het einde van een been te bepalen op basis van een scanresolutie van 500 ppi.

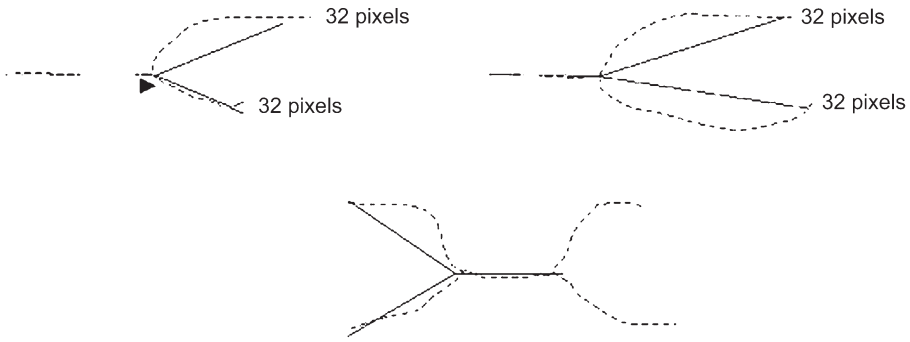
Het eindpunt wordt bepaald in volgorde van voorkomen. De pixels worden berekend op basis van een scanresolutie van 500 ppi. Een andere scanresolutie zou een ander resultaat van de pixelberekening opleveren.

— Afstand is 0,064" (de 32e pixel).

— Eindpunt van het skeletbeen is gelegen tussen 0,02" tot 0,064" (de 10e tot de 32e pixel); er worden geen kortere benen gebruikt.

— Een tweede bifurcatie komt voor op een afstand van 0,064" (voor de 32e pixel).

Figuur 6.1.2



De hoek van de minutiae wordt bepaald door vanuit het splitsingspunt drie virtuele stralen te projecteren tot aan het einde van elk been. De kleinste van de drie door deze stralen gevormde hoeken wordt gesneden om de richting van de minutiae aan te geven.

6.1.3. Assenstelsel

De minutiae van een vingerafdruk worden uitgedrukt door middel van een cartesisch assenstelsel. De locaties van minutiae worden weergegeven door hun x- en y-assen. Het assenstelsel vertrekt vanuit de linkerbovenhoek van het oorspronkelijke beeld, waarbij de x-as rechts omhoog en de y-as naar beneden loopt. Zowel de x- als de y-as van een minutia wordt in pixeleenheden vanuit het vertrekpunt weergegeven. Opgemerkt zij dat de locatie van het vertrekpunt en de meeteenheden niet overeenkomen met de conventie die in de definities van type 9 in ANSI/NIST-ITL 1-2000 wordt gehanteerd.

6.1.4. Richting van de minutiae

Hoeken worden in een standaard wiskundige vorm uitgedrukt, met nul graden rechts en hoekvergrotingen tegen de wijzers van de klok in. De richting van geregistreerde hoeken is, bij eindigende lijnen, achterwaarts langs de lijn en, bij bifurcaties, naar het midden van de „voren". Deze conventie staat diametraal tegenover de conventie voor hoeken in de definities van type 9 in ANSI/NIST-ITL 1-2000.

6.2. *Velden voor logische-recordtype 9 in INCITS-378 Format*

Alle velden van type-9 records worden als ASCII-tekst geregistreerd. In deze tagged-field record mogen geen binaire velden worden gebruikt.

6.2.1. Veld 9.001: logische-recordlengte (Logical Record Length — LEN)

Dit verplichte ASCII-veld bevat de lengte van de logische record en specificeert het totale aantal bytes, daaronder begrepen elk karakter van elk veld in de record.

6.2.2. Veld 9.002: beeldkarakterisering (Image Designation Character — IDC)

Dit verplichte veld van 2 bytes wordt gebruikt om de minutiaegegevens te identificeren en te lokaliseren. De IDC in dit veld moet overeenkomen met de IDC in het bestandsinhoudveld van de type-1 record.

6.2.3. Veld 9.003: afdruktype (IMP)

In dit verplichte veld van 1 byte wordt aangegeven op welke wijze de vingerafdrukgegevens zijn verkregen. In dit veld wordt het afdruktype aangegeven door middel van de ASCII-waarde van de desbetreffende code uit tabel 4.

6.2.4. Veld 9.004: formaat van de minutiae (Minutiæ format — FMT)

Dit veld bevat een „U", die aangeeft dat de vorm van de minutiae gebaseerd is op de norm M1-378. Informatie mag worden gecodeerd volgens de norm M1-378, maar alle gegevensvelden van de type-9 record moeten als ASCII-tekstveld blijven staan.

6.2.5. Veld 9.126: CBEFF-gegevens (Common Biometric Exchange File Format)

Dit veld bevat drie soorten gegevens. Het eerste gegeven is de waarde „27" (0x1B). Dit is de identificatie van de „eigenaar" van het CBEFF die door de International Biometric Industry Association (IBIA) is toegewezen aan technisch comité M1 van de INCITS (InterNational Committee for Information Technology Standards). Het teken <Verenigde Staten> scheidt dit item van de CBEFF Format Type, waaraan de waarde „513" (0x0201) wordt

toegekend om aan te geven dat deze record alleen gegevens over de locatie en de hoekrichting bevat, zonder Extended Data Block-informatie. Het teken <Verenigde Staten> scheidt dit item van de CBEFF Product Identifier (PID), waarmee de „eigenaar" van de coderingsapparatuur wordt geïdentificeerd. Deze waarde wordt door de verkoper bepaald, en is te vinden op de website van de IBIA (www.ibia.org), voor zover ze daarop is bekendgemaakt.

6.2.6. Veld 9.127: identificatie van de afnameapparatuur

Dit veld bevat twee informatie-elementen, gescheiden door het teken <Verenigde Staten>. Het eerste informatie-element is „APPF" indien de apparatuur die oorspronkelijk voor de afname van de afdruk is gebruikt, gecertificeerd is en voldoet aan de eisen van aanhangsel F (IAFIS Image Quality Specification van 29 januari 1999) van CJIS-RS-0010, de specificaties inzake elektronische transmissie van vingerafdrukken van het FBI. Indien de apparatuur niet daaraan voldoet, is de waarde „NONE". Het tweede informatie-element is de identificatie van de afname-apparatuur, in casu een door de verkoper toegewezen productnummer van de afnameapparatuur. Indien de waarde „0" is, betekent dit dat de identificatie van de afnameapparatuur niet bekend is.

6.2.7. Veld 9.128: lengte horizontale lijn (Horizontal Line Length — HLL)

Dit verplichte ASCII-veld bevat het aantal pixels op één enkele horizontale lijn in het doorgezonden beeld. Het maximumaantal pixels op één horizontale lijn is beperkt tot 65 534.

6.2.8. Veld 9.129: lengte verticale lijn (Vertical Line Length — VLL)

Dit verplichte ASCII-veld bevat het aantal horizontale lijnen in het doorgezonden beeld. Het maximumaantal pixels op één verticale lijn is beperkt tot 65 534.

6.2.9. Veld 9.130: schaaleenheden (Scale units — SLC)

In dit verplichte ASCII-veld wordt gespecificeerd welke eenheden zijn gebruikt om de samplefrequentie van het beeld weer te geven (pixeldensiteit). Een „1" in dit veld staat voor pixels per inch, terwijl een „2" voor pixels per centimeter staat. Een „0" in dit veld betekent dat geen schaal is opgegeven. In casu levert het quotiënt van HPS en VPS de pixel-aspect-verhouding op.

6.2.10. Veld 9.131: horizontale pixelschaal (Horizontal pixel scale — HPS)

In dit verplichte ASCII-veld wordt de pixeldensiteit, uitgedrukt in gehele getallen, gespecificeerd die in de horizontale richting wordt gebruikt, voor zover de SLC de waarde „1" of „2" bevat. In alle andere gevallen wordt hiermee de horizontale component van de pixel-aspect-verhouding weergegeven.

6.2.11. Veld 9.132: verticale pixelschaal (Vertical pixel scale — VPS)

In dit verplichte ASCII-veld wordt de pixeldensiteit, uitgedrukt in gehele getallen, gespecificeerd die in de verticale richting wordt gebruikt, voor zover de SLC de waarde „1" of „2" bevat. In alle andere gevallen wordt hiermee de verticale component van de pixel-aspect-verhouding weergegeven.

6.2.12. Veld 9.133: vinger view

Dit verplichte veld bevat het viewnummer van de vinger dat bij de gegevens van deze record hoort. Het viewnummer begint met „0" en loopt telkens met 1 op tot „15".

6.2.13. Veld 9.134: vingerpositie (Finger Position — FGP)

Dit veld bevat de code waarmee de positie van de vinger wordt aangeduid die de informatie in deze type-9 record heeft opgeleverd. Voor het aanduiden van de vinger- of handpalmpositie wordt een code van 1 tot 10 (zie tabel 5) of een handpalmcode (zie tabel 10) gebruikt.

6.2.14. Veld 9.135: vingerkwaliteit

Dit veld geeft de kwaliteit aan van de algemene gegevens van de minutiae van een vinger, en heeft een waarde van 0 tot 100. Dit getal is een algemene aanduiding van de kwaliteit van de vingerrecord, en staat voor de kwaliteit van het oorspronkelijke beeld, van de munitia-extractie en van andere handelingen die gevolgen kunnen hebben voor de munitiae-record.

6.2.15. Veld 9.136: aantal minutiae

Dit verplichte veld bevat een telling van het aantal minutiae dat in deze logische record is vastgelegd.

6.2.16. Veld 9.137: gegevens van de vingerminutiae

Dit verplichte veld bevat zes informatie-elementen, gescheiden door het teken <Verenigde Staten>. Het bestaat uit verschillende subvelden die elk de gegevens van afzonderlijke minutiae bevatten. Het totale aantal minutiaesubvelden moet overeenstemmen met het totaal in veld 136. Het eerste informatie-element is het indexnummer van de minutiae, dat begint bij „1" en met „1" wordt vermeerderd voor elke extra minutia in de vingerafdruk. Het tweede en het derde informatie-element zijn de „x"- en „y"-assen van de minutiae, uitgedrukt in pixeleenheden. Het vierde informatie-element is de hoek van de minutiae, geregistreerd in eenheden van telkens twee graden. Deze waarde is niet-negatief en gaat van 0 tot 179. Het vijfde informatie-element is het soort minutiae. De waarde „0" komt overeen met minutiae van het soort „OTHER" („overige"), terwijl de waarde „1" overeenkomt met een eindigende lijn en de waarde „2" met een vertakkende lijn. Het zesde informatie-element geeft de kwaliteit van de minutiae weer. Deze waarde gaat van minimaal 1 tot maximaal 100. De waarde „0" geeft aan dat geen kwaliteitsoordeel kan worden gegeven. Elk subveld wordt van het volgende subveld gescheiden door middel van het scheidingsteken <RS>.

6.2.17. Veld 9.138: informatie over het lijnental („ridge count")

Dit veld bestaat uit een serie subvelden die elk drie informatie-elementen bevatten. Het eerste informatie-element in het eerste subveld geeft de wijze van extractie van het lijnental aan. Een „0" betekent dat niets bekend is over de wijze van extractie van het lijnental, noch over hun volgorde in de record. Een „1" betekent dat voor elke middelste minutia gegevens over het lijnental zijn verkregen aan de hand van de dichtstbij gelegen minutiae in vier kwadranten, en dat de lijnentallen van alle middelste minutiae samen zijn opgenomen. Een „2" betekent dat voor elke middelste minutia gegevens over het lijnental zijn verkregen aan de hand van de dichtstbij gelegen minutiae in acht octanten, en dat de lijnentallen van alle middelste minutiae samen zijn opgenomen. De twee andere informatie-elementen van het eerste subveld bevatten beide de waarde „0". De informatie-elementen worden gescheiden door het scheidingsteken <Verenigde Staten>. De volgende subvelden bevatten het verhoudingscijfer van de middelste minutiae als eerste informatie-element, het verhoudingscijfer van de nabijgelegen minutiae als tweede informatie-element en het aantal gekruiste lijnen als derde informatie-element. Subvelden worden van elkaar gescheiden door het scheidingsteken <RS>.

6.2.18. Veld 9.139: informatie over de kern

Dit veld bestaat uit een subveld voor elke kern op de oorspronkelijke afbeelding. Elk subveld bestaat uit drie informatie-elementen. De eerste twee elementen bevatten de „x"- en „y"-asposities, uitgedrukt in pixeleenheden. Het derde informatie-element bevat de kernhoek, gemeten in eenheden van 2 graden. Deze waarde is niet-negatief en gaat van 0 tot 179. Verschillende kernen worden van elkaar gescheiden door het scheidingsteken <RS>.

6.2.19. Veld 9.140: informatie over de delta

Dit veld bestaat uit een subveld voor elke delta op de oorspronkelijke afbeelding. Elk subveld bestaat uit drie informatie-elementen. De eerste twee elementen bevatten de „x"- en „y"-asposities, uitgedrukt in pixeleenheden. Het derde informatie-element bevat de deltahoek, gemeten in eenheden van 2 graden. Deze waarde is niet-negatief en gaat van 0 tot 179. Verschillende kernen worden van elkaar gescheiden door het scheidingsteken <RS>.

7. ***Recordtype 13: sporenbeeld in variabele resolutie***

De tagged-field type-13 logische record bevat beeldgegevens van sporenafbeeldingen. Deze beelden worden naar de bevoegde diensten doorgestuurd, waar deze automatisch worden „geëxtraheerd" of door personeel worden bewerkt zodat de gewenste informatie uit de beelden kan worden afgescheiden.

De record bevat informatie over de gebruikte scanresolutie, de beeldgrootte en andere parameters die voor de verwerking van het beeld nodig zijn, vastgelegd in de vorm van tagged-fields.

Tabel 7: vorm van recordtype 13 (sporenbeeld in variabele resolutie)

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	—

Legende: N = numeriek; A = alfabetisch; AN = alfanumeriek; B = binair.

7.1. *Velden voor logische-recordtype 13*

In de volgende alinea's wordt beschreven welke gegevens in de verschillende velden van logische-recordtype 13 worden opgenomen.

In een logische record van type 13 wordt informatie in genummerde velden verstrekt. De eerste twee velden van deze record moeten worden gerangschikt, en het veld met de beeldgegevens dient het laatste fysieke veld in de record te zijn. Tabel 7 bevat per veld van een type-13 record de „voorwaardelijkheidscode", te weten: „M" („mandatory"/verplicht) of „O" („optional"/facultatief), het veldnummer, de veldnaam, de karaktersoort, de veldgrootte en het minimale en maximale aantal keren dat het voorkomt („occurrence limits"). In de laatste kolom staat de maximale bytegrootte van het veld, weergegeven als veldnummer van drie cijfers. Wanneer meer cijfers worden gebruikt voor het veldnummer, zal de maximale bytegrootte navenant stijgen. De twee gegevens in de „field size per occurrence" omvatten ook alle karakterscheidingstekens die in het betreffende veld worden gebruikt. Het „totale aantal bytes" bevat het veldnummer, de informatie en alle scheidingstekens, inclusief het teken „GS".

7.1.1. Veld 13.001: logische-recordlengte (Logical Record Length — LEN)

Dit verplichte ASCII-veld bevat het totale aantal bytes in de type 13-logische record. In veld 13.001 wordt de lengte van de record aangegeven, met inbegrip van elk karakter van elk veld in de record, en de informatiescheidingstekens.

7.1.2. Veld 13.002: beeldkarakterisering (Image Designation Character — IDC)

Dit verplichte ASCII-veld wordt gebruikt om de gegevens van het sporenbeeld in de record te identificeren. Deze IDC komt overeen met de IDC in het bestandsinhoudveld (CNT) van de type-1 record.

7.1.3. Veld 13.003: afdruktype (Impression type — IMP)

Dit verplichte ASCII-veld van één of twee bytes bevat een beschrijving van de wijze waarop het sporenbeeld is verkregen. Dit veld bevat de sporencode, die wordt gekozen uit tabel 4 (vinger) of tabel 9 (handpalm).

7.1.4. Veld 13.004: dienst van herkomst (Source agency/ORI (SRC))

Dit verplichte ASCII-veld bevat de identificatie van de overheidsdienst of organisatie waarvan de foto in de record oorspronkelijk afkomstig is. Normaliter bevat dit veld de identificatie van de dienst van herkomst (Originating Agency Identifier — ORI) van de dienst waar de foto is vastgelegd. Het bestaat uit twee informatie-elementen van het volgende formaat: CC/dienst.

Het eerste informatie-element is de Interpol-landencode (twee alfanumerieke karakters). Het tweede element, de dienst, is een identificatie van de dienst in vrije tekst met ten hoogste 32 alfanumerieke karakters.

7.1.5. Veld 13.005: datum van vastlegging van de sporen (Latent capture date — LCD)

Dit verplichte ASCII-veld bevat de datum waarom het sporenbeeld in de record is vastgelegd. De datum wordt als volgt weergegeven in acht cijfers: CCYYMMDD; CCYY staat voor het jaar waarin het beeld is vastgelegd; MM voor de tientallen en eenheden van de maand, en DD voor de tientallen en eenheden van de dag van de maand. Bijvoorbeeld: 20000229 = 29 februari 2000. De volledige datum moet een geldige datum zijn.

7.1.6. Veld 13.006: lengte horizontale lijn (Horizontal Line Length — HLL)

Dit verplichte ASCII-veld bevat het aantal pixels op één enkele horizontale lijn in het doorgezonden beeld.

7.1.7. Veld 13.007: lengte verticale lijn (Vertical Line Length — VLL)

Dit verplichte ASCII-veld bevat het aantal horizontale lijnen in het doorgezonden beeld.

7.1.8. Veld 13.008: schaaleenheden (Scale units — SLC)

In dit verplichte ASCII-veld wordt gespecificeerd welke eenheden zijn gebruikt om de samplefrequentie van het beeld weer te geven (pixeldensiteit). Een „1” in dit veld staat voor pixels per inch, terwijl een „2” voor pixels per centimeter staat. Een „0” in dit veld betekent dat geen schaal is opgegeven. In casu levert het quotiënt van HPS en VPS de pixel-aspect-verhouding op.

7.1.9. Veld 13.009: horizontale pixelschaal (Horizontal pixel scale — HPS)

In dit verplichte ASCII-veld wordt de pixeldensiteit, uitgedrukt in gehele getallen, gespecificeerd die in de horizontale richting wordt gebruikt, voor zover de SLC de waarde „1” of „2” bevat. In alle andere gevallen wordt hiermee de horizontale component van de pixel-aspect-verhouding weergegeven.

7.1.10. Veld 13.010: verticale pixelschaal (Vertical pixel scale — VPS)

In dit verplichte ASCII-veld wordt de pixeldensiteit, uitgedrukt in gehele getallen, gespecificeerd die in de verticale richting wordt gebruikt, voor zover de SLC de waarde „1” of „2” bevat. In alle andere gevallen wordt hiermee de verticale component van de pixel-aspect-verhouding weergegeven.

7.1.11. Veld 13.011: comprimeringsalgoritme (CGA)

In dit verplichte ASCII-veld wordt aangegeven welke algoritme is gebruikt om de grijswaardenbeelden te comprimeren. Zie aanhangsel 7 voor de comprimeringscodes.

7.1.12. Veld 13.012: bits per pixel (BPX)

Dit verplichte ASCII-veld bevat het aantal bits dat wordt gebruikt om een pixel weer te geven. Dit veld bevat een waarde van „8” voor normale grijswaarden van „0” tot „255”. Elke waarde groter dan „8” in dit veld geeft een grijswaardepixel met grotere precisie weer.

7.1.13. Veld 13.013: vinger/handpalmpositie (FGP)

Dit verplichte tagged-field bevat een of meer mogelijke vinger- of handpalmposities die met het sporenbeeld kunnen overeenkomen. De decimale code die met de gekende of meest voor de hand liggende vingerpositie overeenkomt, staat in tabel 5 en de code die met de meest waarschijnlijke handpalmpositie overeenkomt, in tabel 10; deze codes worden als ASCII-subveld van één of twee karakters opgenomen. Andere vinger- en/of handpalmposities kunnen worden opgegeven door de desbetreffende positiecodes als subvelden op te nemen, gescheiden door het teken „RS”. De code „0”, voor „onbekende vinger”, wordt gebruikt voor elke vingerpositie van één tot tien. De code „20”, voor „onbekende handpalm”, wordt gebruikt voor elke opgenomen handpalmpositie.

7.1.14. Veld 13.014-019: voorbehouden voor toekomstige definities (Reserved for future definition — RSV)

Deze velden zijn voorbehouden voor het opnemen van toekomstige herzieningen van deze norm. In dit stadium van herziening worden deze velden niet gebruikt. Indien deze velden voorkomen, moeten zij worden genegeerd.

7.1.15. Veld 13.020: opmerking (Comment — COM)

Dit facultatieve veld kan worden gebruikt om opmerkingen of andere informatie in ASCII-tekst op te nemen bij de gegevens van het sporenbeeld.

7.1.16. Veld 13.021-199: voorbehouden voor toekomstige definities (Reserved for future definition — RSV)

Deze velden zijn voorbehouden voor het opnemen van toekomstige herzieningen van deze norm. In dit stadium van herziening worden deze velden niet gebruikt. Indien deze velden voorkomen, moeten zij worden genegeerd.

7.1.17. Veld 13.200-998: gebruikergebonden velden (User-defined fields — UDF)

Dit zijn door de gebruiker te definiëren velden die voor toekomstige eisen zullen worden gebruikt. De omvang en inhoud worden door de gebruiker bepaald, in samenspraak met de ontvangende dienst. Indien deze velden worden gebruikt, bevatten zij gegevens in ASCII-tekst.

7.1.18. Veld 13.999: beeldgegevens (DAT)

Dit veld bevat alle gegevens van het afgenomen sporenbeeld. Het krijgt steeds veldnummer 999 en moet altijd het laatste fysieke veld in de record zijn. Zo wordt „13.999:" gevolgd door beeldgegevens, binair weergegeven.

Normaliter wordt elke pixel van niet-gecomprimeerde grijswaardengegevens gequantiseerd tot acht bits (256 grijsniveaus) in één byte. Indien de inhoud van BPX-veld 13.012 groter of kleiner is dan „8", zal het aantal bytes dat nodig is om een pixel te bevatten verschillend zijn. In het geval van comprimering worden de pixelgegevens gecomprimeerd met behulp van de in het GCA-veld gespecificeerde comprimeringstechniek.

7.2. *Einde van recordtype 13: sporenbeeld in variabele resolutie*

Ter wille van de samenhang wordt onmiddellijk na de laatste databyte van veld 13.999 een „FS"-scheidingsteken gebruikt als afscheiding van de volgende logische record. Dit scheidingsteken moet worden meegerekend in de veldlengte van een type-13 record.

8. ***Recordtype 15: handpalmafdrukbeeld in variabele resolutie***

De tagged-field type-15 logische record bevat gegevens over het handpalmafdrukbeeld en wordt gebruikt om deze gegevens uit te wisselen, samen met vaste en gebruikergebonden tekstinformatievelden die bij het gedigitaliseerde beeld horen. De record bevat informatie over de gebruikte scanresolutie, de beeldgrootte en andere parameters of opmerkingen die voor de verwerking van het beeld nodig zijn, vastgelegd in de vorm van tagged-fields. Wanneer handpalmafdrukbeelden naar andere diensten worden doorgezonden, worden deze door de ontvangende diensten verwerkt zodat daaruit de informatie kan worden gewonnen die nodig is om een overeenkomst te kunnen vaststellen.

De beeldgegevens worden rechtstreeks van de betrokkene verkregen door middel van een live-scanapparaat, dan wel een handpalmafdrukkaart of andere media waarop de handpalmafdruk van de betrokkene staat.

De methodes die voor de afname van handpalmafdrukbeelden worden gebruikt, moeten een reeks beelden voor elke hand mogelijk maken. Deze reeks omvat de zijkant van de hand (het deel onder de pink) als gescand beeld, en de volledige handpalm, gaande van de pols tot de vingertippen in een of twee gescande beelden. Indien de volledige handpalm in twee beelden wordt weergegeven, gaat het onderste beeld van de pols tot de bovenkant van het interdigitale gebied (derde vingergewricht), met inbegrip van de duimmuis (thenar) en de pinkmuis (hypothenar). Het bovenste beeld gaat van de onderkant van het interdigitale gebied tot de bovenkant van de vingertoppen. Zo ontstaat een voldoende grote overlapping tussen de twee beelden over het interdigitale gebied van de handpalm. Het matchen van de lijnstructuur en de details in deze gemeenschappelijke zone levert een onderzoeker genoegzaam bewijs dat de beide beelden van dezelfde handpalm afkomstig zijn.

Aangezien een handpalmafdrukopdracht voor verschillende doeleinden kan worden gebruikt, kan deze een of meer unieke afbeeldingen van de handpalm of hand bevatten. Een volledige handpalmafdrukrecordreeks voor een individu bevat normaliter de beelden van de zijkant van de hand (het deel onder de pink) en de volledige handpalm van elke hand. Aangezien een tagged-field logische-beeldrecord slechts één binair veld bevat, is er voor elke zijkant van de hand (het deel onder de pink) een aparte type-15 record nodig en één of twee type-15 records voor elke volledige handpalm. Er zijn dus vier tot zes type-15 records nodig om de handpalmafdrukken van de betrokkene weer te geven bij een normale handpalmafdrukopdracht.

8.1. *Velden voor logische-recordtype 15*

In de volgende alinea's wordt beschreven welke gegevens in de verschillende velden van logische-recordtype 15 worden opgenomen.

In een logische record van type 15 wordt informatie in genummerde velden verstrekt. De eerste twee velden van deze record moeten worden gerangschikt, en het veld met de beeldgegevens dient het laatste fysieke veld in de record te zijn. Tabel 8 bevat per veld van een type-15 record de „voorwaardelijkheidscode", te weten: „M" („mandatory"/verplicht) of „O" („optional"/facultatief), het veldnummer, de veldnaam, de karaktersoort, de veldgrootte en het minimale en maximale aantal keren dat het voorkomt („occurrence limits"). In de laatste kolom staat de maximale bytegrootte van het veld, weergegeven als veldnummer van drie cijfers. Wanneer meer cijfers worden gebruikt voor het veldnummer, zal de maximale bytegrootte navenant stijgen. De twee gegevens in de „field size per occurrence" omvatten ook alle karakterscheidingstekens die in het betreffende veld worden gebruikt. Het „totale aantal bytes" bevat het veldnummer, de informatie en alle karakterscheidingstekens, inclusief het teken „GS".

8.1.1. Veld 15.001: logische-recordlengte (Logical Record Length — LEN)

Dit verplichte ASCII-veld bevat het totale aantal bytes in de type 15-logische record. In veld 15.001 wordt de lengte van de record aangegeven, met inbegrip van elk karakter van elk veld in de record, en de informatiescheidingstekens.

8.1.2. Veld 15.002: beeldkarakterisering (Image Designation Character — IDC)

Dit verplichte ASCII-veld wordt gebruikt om het handpalmafdrukbeeld in de record te identificeren. Deze IDC komt overeen met de IDC in het bestandsinhoudveld (CNT) van de type-1 record.

8.1.3. Veld 15.003: afdruktype (IMP)

Dit verplichte ASCII-veld van 1 byte bevat een beschrijving van de wijze waarop het handpalmafdrukbeeld is verkregen. In dit veld wordt de overeenkomstige code uit tabel 9 ingevoerd.

8.1.4. Veld 15.004: dienst van herkomst (Source agency/ORI (SRC))

Dit verplichte ASCII-veld bevat de identificatie van de overheidsdienst of organisatie waarvan de foto (afbeelding gezicht) in de record oorspronkelijk afkomstig is. Normaliter bevat dit veld de identificatie van de dienst van herkomst (Originating Agency Identifier — ORI) van de dienst waar het beeld is vastgelegd. Het bestaat uit twee informatie-elementen van het volgende formaat: CC/dienst.

Het eerste informatie-element is de Interpol-landencode (2 alfanumerieke karakters). Het tweede element, de dienst, is een identificatie van de dienst in vrije tekst met ten hoogste 32 alfanumerieke karakters.

8.1.5. Veld 15.005: datum van afname van de handpalmafdruk (Palmprint capture date — PCD)

Dit verplichte ASCII-veld bevat de datum van afname van het handpalmafdrukbeeld. De datum wordt weergegeven in 8 cijfers, als volgt: CCYYMMDD; CCYY staat voor het jaar waarin het beeld is vastgelegd; MM voor de tientallen en eenheden van de maand, en DD voor de tientallen en eenheden van de dag in de maand. Bijvoorbeeld: 20000229 = 29 februari 2000. De volledige datum moet een geldige datum zijn.

8.1.6. Veld 15.006: lengte horizontale lijn (Horizontal Line Length — HLL)

Dit verplichte ASCII-veld bevat het aantal pixels op één enkele horizontale lijn in het doorgezonden beeld.

8.1.7. Veld 15.007: lengte verticale lijn (Vertical Line Length — VLL)

Dit verplichte ASCII-veld bevat het aantal horizontale lijnen in het doorgezonden beeld.

8.1.8. Veld 15.008: schaaleenheden (Scale units — SLC)

In dit verplichte ASCII-veld wordt gespecificeerd welke eenheden zijn gebruikt om de samplefrequentie van het beeld weer te geven (pixeldensiteit). Een „1" in dit veld staat voor pixels per inch, terwijl een „2" voor pixels per centimeter staat. Een „0" in dit veld betekent dat geen schaal is opgegeven. In casu levert het quotiënt van HPS en VPS de pixel-aspect-verhouding op.

8.1.9. Veld 15.009: horizontale pixelschaal (Horizontal pixel scale — HPS)

In dit verplichte ASCII-veld wordt de pixeldensiteit, uitgedrukt in gehele getallen, gespecificeerd die in de horizontale richting wordt gebruikt, voor zover de SLC de waarde „1" of „2" bevat. In alle andere gevallen wordt hiermee de horizontale component van de pixel-aspect-verhouding weergegeven.

8.1.10. Veld 15.010: verticale pixelschaal (Vertical pixel scale — VPS)

In dit verplichte ASCII-veld wordt de pixeldensiteit, uitgedrukt in gehele getallen, gespecificeerd die in de verticale richting wordt gebruikt, voor zover de SLC de waarde „1" of „2" bevat. In alle andere gevallen wordt hiermee de verticale component van de pixel-aspect-verhouding weergegeven.

Tabel 8: vorm van recordtype 15 (handpalmafdruk in variabele resolutie)

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	—

Tabel 9: Soort handpalmafdruk

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. Veld 15.011: comprimeringsalgoritme (CGA)

In dit verplichte ASCII-veld wordt aangegeven welke algoritme is gebruikt om de grijswaardenbeelden te comprimeren. Indien de waarde in dit veld „NONE" is, betekent dit dat de gegevens in deze record niet zijn gecomprimeerd. Voor beelden die moeten worden gecomprimeerd, bevat dit veld de meest aangewezen methode voor het comprimeren van afdrukbeelden van de tien vingers. Voor de definitie van geldige comprimeringscodes: zie aanhangsel 7.

8.1.12. Veld 15.012: bits per pixel (BPX)

Dit verplichte ASCII-veld bevat het aantal bits dat wordt gebruikt om een pixel weer te geven. Dit veld bevat een waarde van „8" voor normale grijswaarden van „0" tot „255". Elke waarde groter of kleiner dan „8" in dit veld geeft een grijswaardepixel met respectievelijk grotere of kleinere precisie weer.

Tabel 10: handpalmcodes, -zones en -afmetingen

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. Veld 15.013: positie handpalmafdruk (Palmprint position — PLP)

Dit verplichte tagged-field bevat de handpalmafdrukpositie die overeenkomt met het handpalmafdrukbeeld. Het decimale codenummer dat overeenkomt met de gekende of meest waarschijnlijke handpalmafdrukpositie staat in tabel 10 en wordt weergegeven als ASCII-subveld van 2 karakters. Tabel 10 bevat tevens de maximale beeldvlakken en -afmetingen voor elke mogelijke positie van de handpalmafdruk.

8.1.14. Veld 15.014-019: voorbehouden voor toekomstige definities (Reserved for future definition — RSV)

Deze velden zijn voorbehouden voor het opnemen van toekomstige herzieningen van deze norm. In dit stadium van herziening worden deze velden niet gebruikt. Indien deze velden voorkomen, moeten zij worden genegeerd.

8.1.15. Veld 15.020: opmerking (Comment — COM)

Dit facultatieve veld kan worden gebruikt om opmerkingen of andere informatie in ASCII-tekst op te nemen bij de gegevens van het handpalmafdrukbeeld.

8.1.16. Veld 15.021-199: voorbehouden voor toekomstige definities (Reserved for future definition — RSV)

Deze velden zijn voorbehouden voor het opnemen van toekomstige herzieningen van deze norm. In dit stadium van herziening worden deze velden niet gebruikt. Indien deze velden voorkomen, moeten zij worden genegeerd.

8.1.17. Veld 15.200-998: gebruikergebonden velden (User-defined fields — UDF)

Dit zijn door de gebruiker te definiëren velden die voor toekomstige eisen zullen worden gebruikt. De omvang en inhoud worden door de gebruiker bepaald, in samenspraak met de ontvangende dienst. Indien deze velden worden gebruikt, bevatten zij gegevens in ASCII-tekst.

8.1.18. Veld 15.999: beeldgegevens (DAT)

Dit veld bevat alle gegevens van het afgenomen beeld van de handpalmafdruk. Het krijgt steeds veldnummer 999 en moet altijd het laatste fysieke veld in de record zijn. „15.999:" bijvoorbeeld wordt gevolgd door beeldgegevens, binair weergegeven. Normaliter wordt elke pixel van niet-gecomprimeerde grijswaardengegevens gequantiseerd tot acht bits (256 grijsniveaus) in één byte. Indien de inhoud van BPX-veld 15.012 groter of kleiner is dan „8", zal het aantal bytes dat nodig is om een pixel te bevatten verschillend zijn. In het geval van comprimering worden de pixelgegevens gecomprimeerd met behulp van de in het CGA-veld gespecificeerde comprimeringstechniek.

8.2. *Einde van recordtype 15: handpalmafdrukbeeld in variabele resolutie*

Ter wille van de samenhang wordt onmiddellijk na de laatste databyte van veld 15.999 een „FS"-scheidingsteken gebruikt als afscheiding van de volgende logische record. Dit scheidingsteken moet worden meegerekend in de veldlengte van een type-15 record.

8.3. *Andere records van type 15 (handpalmafdrukbeelden in variabele resolutie)*

Het bestand kan nog andere type-15 records bevatten. Voor elk extra handpalmafdrukbeeld is een volledige type-15 logische record en een „FS"-scheidingsteken vereist.

Tabel 11: maximumaantal ter verificatie geaccepteerde mogelijke „hits" per transmissie

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

Soorten zoekopdrachten:

TP/TP: volledige afdruk (tien vingers) in bestand van volledige afdrukken (tien vingers)

LT/TP: vingerafdrukspoor in bestand van volledige afdrukken (tien vingers)

LP/PP: handpalmafdrukspoor in bestand van handpalmafdrukken

TP/UL: volledige afdruk (tien vingers) in bestand van onopgeloste vingerafdruksporen

LT/UL: vingerafdrukspoor in bestand van onopgeloste vingerafdruksporen

PP/ULP: handpalmafdruk in bestand van onopgeloste handpalmafdruksporen

LP/ULP: handpalmafdrukspoor in bestand van onopgeloste handpalmafdruksporen

9. ***Aanhangsels bij hoofdstuk 2 (uitwisseling van dactyloscopische gegevens)***

9.1. *Aanhangsel 1 — Codes ASCII-scheidingstekens*

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
Verenigde Staten	1/15	Separates individual information items of the field or subfield

([1]) Dit is de positie zoals gedefinieerd in de ASCII-norm.

9.2. *Aanhangsel 2 — Berekening alfanumeriek controlekarakter*

Voor TCN en TCR (velden 1.09 en 1.10):

Het getal dat overeenkomt met het controlekarakter wordt met de volgende formule verkregen:

(YY * 10^8 + SSSSSSSS) Modulo 23

waarbij YY en SSSSSSSS de numerieke waarden zijn van respectievelijk de laatste twee cijfers van het jaar en het serienummer.

Aan de hand daarvan wordt het controlekarakter verkregen op basis van navolgende overzichtstabel.

Voor CRO (veld 2.010)

Het getal dat overeenkomt met het controlekarakter wordt met de volgende formule verkregen:

(YY * 10^6 + NNNNNN) Modulo 23

waarbij YY en NNNNNN de numerieke waarden zijn van respectievelijk de laatste twee cijfers van het jaar en het serienummer.

Aan de hand daarvan wordt het controlekarakter verkregen op basis van navolgende overzichtstabel.

Overzichtstabel controlekarakters

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. *Aanhangsel 3 — Karaktercodes*

7-bit ANSI-code voor de onderlinge uitwisseling van informatie

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. *Aanhangsel 4 — Overzicht opdrachten*

Type-1 record (verplicht)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Kolom voorwaardelijkheidsindicatie:

O = „optional" (facultatief); M = „mandatory" (verplicht); C = voorwaarde in het geval van een antwoord aan de dienst van herkomst

Type-2 record (verplicht)

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	—	—

Kolom voorwaardelijkheidsindicatie:

O = „optional" (facultatief); M = „mandatory" (verplicht); C = „Conditional" (voorwaarde) indien data beschikbaar zijn

* = indien de gegevenstransmissie op de nationale wetgeving is gebaseerd (en niet onder Besluit 2008/615/JBZ valt)

9.5. *Aanhangsel 5 — definities type-1 record*

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{Verenigde Staten}15{RS}2{Verenigde Staten}00{RS}4{Verenigde Staten}01{RS}4{Verenigde Staten}02{RS}4{Verenigde Staten}03{RS}4{Verenigde Staten}04{RS}4{Verenigde Staten}05{RS}4{Verenigde Staten}06{RS}4{Verenigde Staten}07{RS}4{Verenigde Staten}08{RS}4{Verenigde Staten}09{RS}4{Verenigde Staten}10{RS}4{Verenigde Staten}11{RS}4{Verenigde Staten}12{RS}4{Verenigde Staten}13{RS}4{Verenigde Staten}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{Verenigde Staten}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Kolom voorwaardelijkheidsindicatie: O = „Optional" (facultatief), M = „Mandatory" (verplicht), C = „Conditional" (voorwaarde)

Kolom karaktertype: A = alfanumeriek, N = numeriek, B = binair

1* toegestane karakters voor de benaming van de dienst zijn [„0..9", „A..Z", „a..z", „_", „.", „", „-"]

9.6. *Aanhangsel 6 — Definities type-2 record*

Tabel A.6.1: CPS- en PMS-opdracht

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}

Tabel A.6.2: SRE-opdracht

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}

Tabel A.6.3: ERR-opdracht

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}

Tabel A.6.4: MPS- en MMS-opdracht

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}

Kolom voorwaardelijkheidsindicatie: O = „Optional" (facultatief), M = „Mandatory" (verplicht), C = „Conditional" (voorwaarde)

Kolom karaktertype: A = alfanumeriek, N = numeriek, B = binair

1* toegestane karakters zijn [„0..9", „A..Z", „a..z", „_","„.", " ", „-"," ,"]

9.7. *Aanhangsel 7 — Grijswaardencomprimeringscodes*

Comprimeringscodes

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

9.8. *Aanhangsel 8 — Mailspecificatie*

Voor een betere interne werkorganisatie moeten in de „betreft"-regel van een e-mailbericht over een PRUEM-opdracht de landencode (CC) van de lidstaat van verzending van het bericht en het soort opdracht (Type of Transaction — TOT, veld 1.004) worden ingevuld.

Formaat: CC/soort opdracht

Voorbeeld: „DE/CPS"

De „body" van het e-mailbericht mag leeg worden gelaten.

HOOFDSTUK 3: **Uitwisseling van gegevens uit kentekenregisters**

1. ***Gemeenschappelijke datareeks voor geautomatiseerde bevraging van gegevens uit kentekenregisters***

1.1. *Definities*

De verplichte en de facultatieve gegevenselementen bedoeld in artikel 16, lid 4, worden als volgt gedefinieerd:

„Mandatory" (M) (verplicht):

De gegevens moeten worden verstrekt wanneer de informatie beschikbaar is in een nationaal register van de lidstaat. Er bestaat dus een verplichting om de informatie uit te wisselen indien deze beschikbaar is.

„Optional" (O) (facultatief):

De gegevens mogen worden verstrekt wanneer de informatie beschikbaar is in een nationaal register van de lidstaat. Het is dus niet verplicht de informatie uit te wisselen, zelfs wanneer deze beschikbaar is.

Elementen in de datareeks die een specifiek belang hebben voor de toepassing van Besluit 2008/615/JBZ, krijgen elk de vermelding Y.

1.2. *Bevraging voertuig/eigenaar/houder*

1.2.1. Inleiden van de bevraging

Informatie kan op twee verschillende manieren worden bevraagd:

— op grond van chassisnummer (VIN), referentiedatum en tijdstip (facultatief);

— op grond van kentekennummer, chassisnummer (VIN) (facultatief), referentiedatum en tijdstip (facultatief).

Aan de hand van deze bevragingscriteria zal informatie over een (of soms meer) voertuig(en) worden teruggestuurd. Indien voor slechts één voertuig informatie moet worden teruggestuurd, worden alle gegevenselementen in één enkel antwoord teruggestuurd. Indien meer dan een voertuig wordt gevonden, kan de aangezochte lidstaat zelf bepalen welke elementen worden teruggestuurd; alle elementen of alleen elementen om de bevraging te verfijnen (bv. omwille van privacyredenen of in verband met de prestaties van het systeem).

De elementen waarmee de bevraging moet worden verfijnd, staan in punt 1.2.2.1. In punt 1.2.2.2 staat de volledige gegevensreeks beschreven.

Bevragingen aan de hand van chassisnummer, referentiedatum en tijdstip kunnen in een of in alle deelnemende lidstaten worden uitgevoerd.

Bevragingen aan de hand van rijbewijsnummer, referentiedatum en tijdstip moeten in één specifieke lidstaat worden uitgevoerd.

Normaliter worden de huidige datum en het huidige tijdstip als maatstaf voor een bevraging genomen, maar er kunnen ook bevragingen met een referentiedatum en -tijdstip in het verleden worden verricht. Indien een bevraging met een referentiedatum en tijdstip in het verleden wordt verricht en in het register van de lidstaat in kwestie geen historische informatie beschikbaar is omdat dergelijke informatie hoegenaamd niet wordt geregistreerd, kan actuele informatie worden teruggestuurd met de vermelding dat het om actuele informatie gaat.

1.2.2. Datareeks

1.2.2.1. Terug te sturen gegevens die noodzakelijk zijn voor het verfijnen van de bevraging

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 (verplicht) voor zover beschikbaar in het nationale register, O = optional (facultatief).
(2) Specifiek door de lidstaten toegekende aanwijzingen worden aangegeven met Y.
(3) Geharmoniseerde documentafkorting, zie Richtlijn 1999/37/EG van de Raad van 29.4.1999.

1.2.2.2. Volledige datareeks

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 holdership 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 holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: — is the vehicle owner — is not the vehicle owner — is not identified by the registration certificate as being the vehicle owner	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y

Item	M/O [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 (verplicht) voor zover beschikbaar in het nationale register, O = optional (facultatief).
(2) Geharmoniseerde documentafkorting, zie Richtlijn 1999/37/EG van de Raad van 29.4.1999.
(3) In Luxemburg worden twee aparte identificatienummers voor kentekendocumenten gebruikt.

2. ***Gegevensbeveiliging***

2.1. *Overzicht*

De Eucaris-softwareapplicatie regelt de beveiligde communicatie met de andere lidstaten en communiceert met de achterliggende systemen van de betreffende lidstaten via XML. Wanneer de lidstaten berichten uitwisselen, verzenden zij deze rechtstreeks naar de ontvanger. De datacentra van de lidstaten zijn met het TESTA-netwerk van de Europese Unie verbonden.

De XML-berichten die over het netwerk worden verzonden, zijn versleuteld door middel van SSL. De berichten die naar de *back-end* worden gezonden, zijn niet versleuteld, aangezien de verbinding tussen de applicatie en de *back-end* in een beveiligde omgeving tot stand wordt gebracht.

De lidstaten kunnen gebruikmaken van de meegeleverde gebruikersinterface om hun eigen register of dat van andere lidstaten te bevragen. Gebruikers worden geïdentificeerd door middel van een gebruikersnaam/-paswoord of een client certificate. De verbinding met de gebruikers kan worden versleuteld, maar dit valt onder de verantwoordelijkheid van de individuele lidstaten.

2.2. *Beveiligingskenmerken in verband met het berichtenverkeer*

Het beveiligingsontwerp is gebaseerd op een combinatie van HTTPS en een XML-handtekening. Bij dit alternatief wordt een XML-handtekening gebruikt voor het ondertekenen van de berichten die naar de server worden verzonden, en kan de verzender van het bericht worden geauthenticeerd door controle van de handtekening. Om de vertrouwelijkheid en integriteit van het verzonden bericht te beschermen, wordt éénzijdige SSL (alleen een servercertificaat) gebruikt, dat tevens bescherming biedt tegen schrapping/herhaling en intrusieaanvallen. In plaats van de ontwikkeling van maatwerksoftware met het oog op tweezijdige SSL, wordt een XML-handtekening geïmplementeerd. Het gebruik van XML-handtekeningen staat dichter bij webdiensten dan tweezijdige SSL en is daarom strategischer.

XML-handtekeningen kunnen op verschillende manieren worden geïmplementeerd; in casu is gekozen voor gebruikmaking van XML-handtekeningen als onderdeel van de WSS (Web Services Security — beveiliging webdiensten). WSS voorziet in een specificatie van het gebruik van XML-handtekeningen. Aangezien WSS gebaseerd is op de SOAP-norm, ligt het voor de hand dat zoveel mogelijk aansluiting wordt gezocht bij deze norm.

2.3. *Andere beveiligingskenmerken dan in verband met het berichtenverkeer*

2.3.1. Authenticatie van gebruikers

Gebruikers van de Eucaris-webapplicatie authenticeren zichzelf door middel van een gebruikersnaam en een paswoord. Aangezien standaard Windows-authenticatie wordt gebruikt, kunnen de lidstaten indien nodig het gebruikersauthenticatieniveau verhogen door client certificates te gebruiken.

2.3.2. Gebruikersrollen

De Eucaris-softwareapplicatie ondersteunt verschillende gebruikersrollen. Elk dienstencluster heeft zijn eigen authorisatie. (Exclusieve) gebruikers van de „Eucaris verdragsfunctionaliteit" mogen bijvoorbeeld de „Prüm-functionaliteit" niet gebruiken. De administratordiensten zijn gescheiden van de reguliere eindgebruikersrollen.

2.3.3. Bewaren en traceren van berichtenverkeer

Het gebruik van de softwareapplicatie Eucaris vergemakkelijkt het bewaren van de verschillende soorten berichten. Door middel van een administratorfunctie kan een nationale administrator bepalen welke berichten worden bewaard: verzoeken van eindgebruikers, inkomende verzoeken van andere lidstaten, informatie uit de nationale registers, enz.

De applicatie kan zodanig worden geconfigureerd dat een interne databank wordt gebruikt voor deze logfunctie, dan wel een externe databank (Oracle). De beslissing over het soort berichten dat moet worden bewaard, hangt duidelijk af van de bewaringsmogelijkheden die elders in de achterliggende systemen en de daarmee verbonden gebruikersapplicaties beschikbaar zijn.

De kop van elk bericht bevat informatie over de verzoekende lidstaat, de verzoekende organisatie in die lidstaat en de betrokken gebruiker. Ook de reden van het verzoek wordt aangegeven.

Door gecombineerde bewaring in de verzoekende en antwoordende lidstaat is het mogelijk het berichtenverkeer volledig te traceren (bv. op verzoek van een betrokken burger).

De bewaring wordt geconfigureerd via de Eucaris gebruikersinterface (menu Beheer, Logging configuratie). De bewaringsfunctionaliteit wordt uitgevoerd door het Core System. Indien is aangegeven dat een bericht moet worden bewaard, wordt het volledige bericht (kop en de eigenlijke berichttekst) in één record opgeslagen. Het bewaringsniveau kan worden vastgesteld per gedefinieerde dienst en per soort bericht dat langs het Core System passeert.

Bewaringsniveaus

De volgende bewaringsniveaus zijn mogelijk:

„Private" (privé) — het bericht wordt bewaard: het bericht is NIET beschikbaar voor extract logging, maar is alleen op nationaal niveau beschikbaar, voor audits en probleemoplossing.

„None" (geen) — het bericht wordt niet bewaard.

Soorten berichten

De informatie-uitwisseling tussen de lidstaten bestaat uit verschillende berichten, waarvan in de navolgende figuur een schematische voorstelling wordt gegeven.

De volgende soorten berichten (in de getoonde figuur voor het Eucaris Core System van lidstaat X) zijn mogelijk:

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

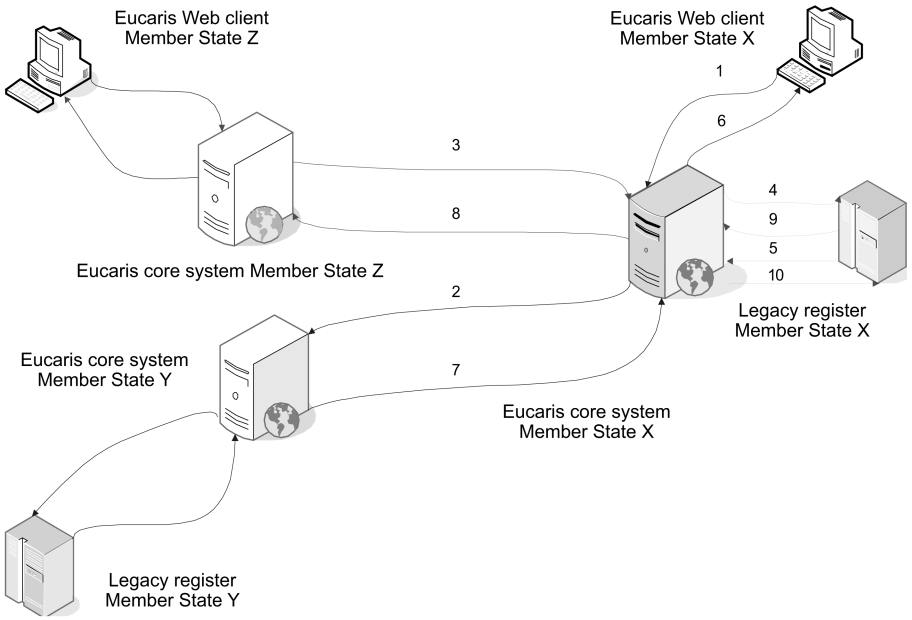
In onderstaande figuur worden de volgende informatie-uitwisselingen veraanschouwelijkt:

— Informatieverzoek van lidstaat X aan lidstaat Y — blauwe pijlen. Dit verzoek, en het antwoord daarop, bestaan uit berichten van respectievelijk de soorten 1, 2, 7 en 6.

— Informatieverzoek van lidstaat Z aan lidstaat X — rode pijlen. Dit verzoek, en het antwoord daarop, bestaan uit berichten van respectievelijk de soorten 3, 4, 9 en 8.

— Informatieverzoek van een ouder register aan het core system (deze route omvat ook een verzoek van een specifieke cliënt achter het oudere register) — groene pijlen. Dit soort verzoek bestaat uit berichten van de soorten 5 en 10.

Figuur: Soort berichten voor bewaring



2.3.4. Hardware beveiligingsmodule

Er wordt geen module voor beveiliging van hardware gebruikt.

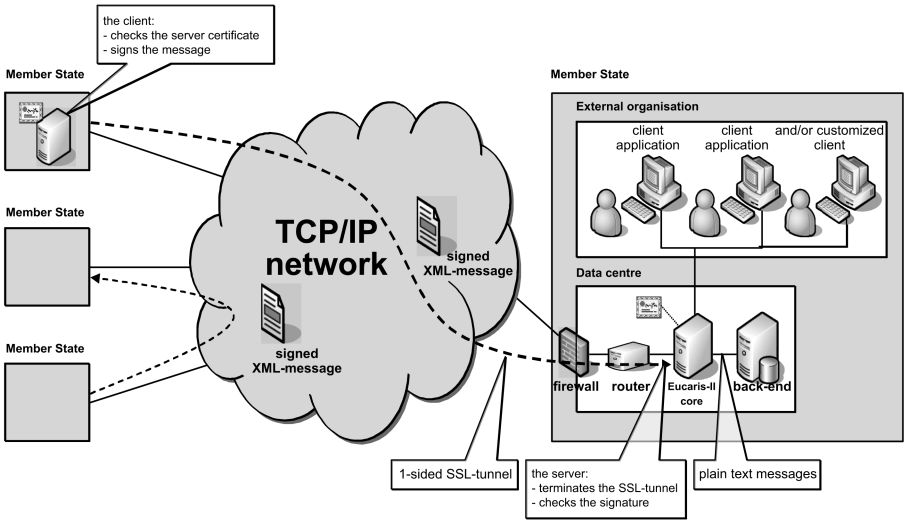
Een Hardware Security Module (HSM — hardware beveiligingsmodule) biedt goede bescherming voor de sleutel die wordt gebruikt om berichten te ondertekenen en servers te identificeren. Dit komt het algemene beveiligingsniveau ten goede, maar de aankoop en het onderhoud van een HSM zijn duur en er zijn geen vereisten die een besluit tot een FIPS 140-2 van niveau 2 of een niveau 3-HSM rechtvaardigen. Aangezien gebruik wordt gemaakt van een gesloten netwerk dat bedreigingen op doeltreffende wijze tegengaat, is besloten in eerste instantie geen HSM te gebruiken. Indien een HSM nodig zou blijken om bijvoorbeeld een accreditatie te verkrijgen, kan deze aan de architectuur worden toegevoegd.

3. *Technische voorwaarden voor de uitwisseling van gegevens*

3.1. *Algemene beschrijving van de EUCARIS-applicatie*

3.1.1. Overzicht

De Eucaris-applicatie verbindt alle deelnemende lidstaten in een vermaasd netwerk waarin elke lidstaat rechtstreeks met een andere lidstaat communiceert. Er is geen centrale component nodig om communicatie tot stand te brengen. De Eucaris-applicatie regelt de beveiligde communicatie met de andere lidstaten en communiceert met de achterliggende systemen van de betreffende lidstaten via XML. Deze architectuur kan als volgt worden veraanschouwelijkt:



Wanneer de lidstaten berichten uitwisselen, verzenden zij deze rechtstreeks naar de ontvanger. De datacentra van de lidstaten zijn verbonden met het netwerk dat voor de uitwisseling van het bericht wordt gebruikt (TESTA). Om toegang te krijgen tot het TESTA-netwerk brengen de lidstaten via hun nationale poort een verbinding met TESTA tot stand. Voor de verbinding met het netwerk wordt een firewall gebruikt; een router verbindt de Eucaris-applicatie met de firewall. Al naargelang de gekozen bescherming van de berichten wordt een certificaat gebruikt door de router of door de Eucaris-applicatie.

De lidstaten kunnen gebruikmaken van de meegeleverde gebruikersinterface om hun eigen register of dat van andere lidstaten te bevragen. Via de gebruikersinterface wordt een verbinding met Eucaris tot stand gebracht. Gebruikers worden geïdentificeerd door middel van een gebruikersnaam/-paswoord of een client certificate. De verbinding met gebruikers in externe organisaties (bv. politie) kan worden versleuteld, maar dit valt onder de verantwoordelijkheid van de individuele lidstaten.

3.1.2. Toepassingsgebied van het systeem

Het toepassingsgebied van Eucaris is beperkt tot de processen die gepaard gaan met de uitwisseling van informatie tussen de voertuigregistratieautoriteiten in de lidstaten en tot een basisweergave van deze informatie. De procedures en geautomatiseerde processen waarin de informatie dient te worden gebruikt, vallen buiten het toepassingsgebied van het systeem.

De lidstaten kunnen ervoor kiezen gebruik te maken van de standaard gebruikersinterface van Eucaris, of een eigen gebruikersinterface te ontwikkelen. In navolgende tabel wordt aangegeven welke aspecten van het Eucaris-systeem verplicht moeten worden gebruikt en/of voorgeschreven, en welke facultatief kunnen worden gebruikt en/of vrij door de lidstaten kunnen worden bepaald.

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 helpdesk functions are managed centrally by an appointed Member State.

[1] M (mandatory) = verplicht te gebruiken of in acht te nemen; O (optional) = facultatief te gebruiken of in acht te nemen.

3.2. *Functionele en niet-functionele eisen*

3.2.1. Algemene functionaliteit

In dit deel worden de belangrijkste algemene functies in algemene bewoordingen beschreven.

Nr.	Beschrijving
1.	Het systeem maakt het de voertuigregistratieautoriteiten van de lidstaten mogelijk interactief vraag- en antwoordberichten uit te wisselen.
2.	Het systeem bevat een gebruikersinterface, waarmee eindgebruikers hun verzoeken kunnen verzenden en waarbij de antwoordinformatie zodanig wordt gepresenteerd dat deze manueel kan worden verwerkt.
3.	Het systeem faciliteert „broadcasting", zodat een lidstaat een verzoek naar alle andere lidstaten kan zenden. De inkomende antwoorden worden door de coreapplicatie tot één antwoordbericht gebundeld, dat naar de gebruikersinterface wordt gezonden (zogeheten „meerlandenbevraging").
4.	Het systeem kan verschillende soorten berichten verwerken. De gebruikersrollen, autorisatie, routing, ondertekening en bewaring worden telkens per specifieke dienst gedefinieerd.
5.	Het systeem maakt het de lidstaten mogelijk reeksen berichten of berichten met een groot aantal verzoeken of antwoorden uit te wisselen. Deze berichten worden asynchroon behandeld.
6.	Het systeem plaatst asynchrone berichten in een wachtrij indien de ontvangende lidstaat tijdelijk niet bereikbaar is, en garandeert de aflevering van het bericht zodra de bestemming opnieuw te bereiken is.
7.	Het systeem slaat inkomende asynchrone berichten op totdat deze kunnen worden verwerkt.
8.	Het systeem verschaft alleen toegang tot de Eucaris-applicaties van de andere lidstaten, en niet tot individuele organisaties in die lidstaten; dit betekent dat elke voertuigregistratieautoriteit als enig netwerktoegangspunt tussen haar nationale eindgebruikers en de overeenstemmende autoriteiten in de andere lidstaten fungeert.
9.	Op één Eucaris-server kunnen gebruikers van verschillende lidstaten worden gedefinieerd en geautoriseerd, conform de rechten van de betrokken lidstaat.
10.	De berichten bevatten informatie over de verzoekende lidstaat, organisatie en eindgebruiker.
11.	Het systeem faciliteert het bewaren van berichtenverkeer tussen de verschillende lidstaten en tussen de coreapplicatie en de nationale registratiesystemen.
12.	Het systeem voorziet in de mogelijkheid dat een specifieke „secretaris" — een organisatie of lidstaat die uitdrukkelijk voor deze taak is aangewezen — vastgelegde informatie over verzonden/ontvangen berichten van alle deelnemende lidstaten verzamelt om statistische rapporten op te stellen.
13.	Elke lidstaat geeft zelf aan welke bewaarde informatie beschikbaar wordt gesteld voor de secretaris, en welke informatie „privé" is.
14.	Het systeem voorziet in de mogelijkheid dat de nationale administrateurs van elke lidstaat gebruiksstatistieken opvragen.
15.	Met eenvoudige administratieve opdrachten kunnen nieuwe lidstaten aan het systeem worden toegevoegd.

3.2.2. Bruikbaarheid

Nr.	Beschrijving
16.	Het systeem biedt een interface voor de geautomatiseerde verwerking van berichten door back-end-systemen/achterliggende systemen en maakt de integratie van de gebruikersinterface in die systemen mogelijk (specifieke gebruikersinterface).
17.	Het systeem is gemakkelijk aan te leren, spreekt voor zichzelf en bevat een helpfunctie.
18.	Bij het systeem hoort documentatie die bedoeld is om de lidstaten bij te staan op het vlak van integratie, operationele activiteiten en toekomstig onderhoud (bv. referentiehandboeken, functionele/technische documentatie, praktische gids, …).
19.	De meertalige gebruikersinterface biedt eindgebruikers de mogelijkheid een voorkeurtaal te selecteren.
20.	De gebruikersinterface voorziet in de mogelijkheid dat een lokale administrator schermitems en gecodeerde informatie in de nationale taal vertaalt.

3.2.3. Betrouwbaarheid

Nr.	Beschrijving
21.	Het systeem is ontworpen als een robuust en betrouwbaar operationeel systeem dat foutieve manipulaties van operatoren kan verdragen en stroomonderbrekingen of andere calamiteiten probleemloos doorstaat. Het systeem moet zonder of met een minimaal verlies aan gegevens opnieuw kunnen worden opgestart.
22.	Het systeem moet stabiele en reproduceerbare resultaten opleveren.
23.	Het systeem is zodanig ontwerpen dat het betrouwbaar functioneert. Het systeem kan worden geïmplementeerd in een configuratie die in elke bilaterale communicatie een beschikbaarheid van 98 % garandeert (door middel van redundantie, het gebruik van back-up servers, enz.).
24.	Het is mogelijk ook delen van het systeem te gebruiken wanneer sommige componenten buiten gebruik zijn (indien lidstaat C niet bereikbaar is, kunnen lidstaten A en B nog altijd met elkaar communiceren). Het aantal zwakke punten (single points of failure) in de informatieketen moet zo klein mogelijk worden gehouden.
25.	De hersteltijd na een ernstig defect moet minder dan één dag zijn. De uitvaltijd moet tot een minimum kunnen worden beperkt door ondersteuning op afstand, bijvoorbeeld door een centrale service desk.

3.2.4. Prestaties

Nr.	Beschrijving
26.	Het systeem kan dag en nacht worden gebruikt. Deze beschikbaarheid (dag en nacht) is bijgevolg ook vereist voor de achterliggende systemen van de lidstaten.
27.	Het systeem antwoordt snel op verzoeken van de gebruiker, ook wanneer terzelfder tijd op de achtergrond andere taken worden uitgevoerd. Deze eis geldt ook voor de achterliggende systemen van de deelnemende partijen, zodat een aanvaardbare antwoordtijd kan worden gegarandeerd. Een algemene antwoordtijd van maximaal 10 seconden voor één enkel verzoek is aanvaardbaar.
28.	Het systeem is als meergebruikerssysteem zodanig ontworpen dat achtergrondtaken kunnen voortgaan terwijl de gebruiker „op de voorgrond" andere taken uitvoert.
29.	Het systeem is zodanig ontworpen dat het schaalbaar is en derhalve een eventuele toename van het aantal berichten als gevolg van de toevoeging van nieuwe functies of nieuwe organisaties of lidstaten aankan.

3.2.5. Beveiliging

Nr.	Beschrijving
30.	Het systeem is geschikt (bv. wat de beveiligingsmaatregelen betreft) voor de uitwisseling van berichten die gevoelige persoonsgegevens (bv. over eigenaars/houders van voertuigen) bevatten die als EU-restricted zijn gerubriceerd.
31.	Het systeem wordt zodanig onderhouden dat ongeoorloofde toegang tot de gegevens wordt voorkomen.
32.	Het systeem voorziet in beheer van de rechten en vergunningen van de nationale eindgebruikers.
33.	De lidstaten kunnen de identiteit van de verzender controleren (op lidstaatniveau) door middel van XML-handtekeningen.
34.	De lidstaten moeten andere lidstaten uitdrukkelijk toestemming geven om specifieke informatie op te vragen.
35.	Het systeem voorziet op applicatieniveau in een volledig beveiligings- en versleutelingsbeleid dat verenigbaar is met het beveiligingsniveau dat in zulke situaties is vereist. Exclusiviteit en integriteit van de informatie worden door het gebruik van XML-handtekeningen gegarandeerd, en versleuteling door middel van SSL-tunnels.
36.	Alle berichtenverkeer kan worden getraceerd door middel van de logboekfunctie.
37.	Er is voorzien in bescherming tegen aanvallen gericht op wissen (een derde wist een bericht) of op herhaling of intrusie (een derde herhaalt of introduceert een bericht).
38.	Het systeem gebruikt TTP-certificaten (Trusted Third Party).
39.	Het systeem kan verschillende certificaten per lidstaat aan, al naargelang het soort bericht of dienst.

Nr.	Beschrijving
40.	Op applicatieniveau zijn voldoende beveiligingsmaatregelen getroffen om niet-geaccrediteerde netwerken te kunnen gebruiken.
41.	Het systeem is voorzien op de nieuwste beveiligingstechnieken, zoals een XML-firewall.

3.2.6. Aanpasbaarheid

Nr.	Beschrijving
42.	Het systeem kan met nieuwe berichten en nieuwe functies worden uitgebreid. Aanpassing vergt minimale kosten. Dit is te danken aan de gecentraliseerde ontwikkeling van applicatiecomponenten.
43.	De lidstaten kunnen nieuwe soorten berichten definiëren voor bilateraal gebruik. Niet alle lidstaten hoeven alle soorten berichten te ondersteunen.

3.2.7. Ondersteuning en onderhoud

Nr.	Beschrijving
44.	Het systeem voorziet in monitoringsmogelijkheden voor een centrale service desk en/of operatoren met betrekking tot het netwerk en de servers in de verschillende lidstaten.
45.	Het systeem voorziet in de mogelijkheid van ondersteuning op afstand door een centrale service desk.
46.	Het systeem voorziet in faciliteiten voor probleemanalyse.
47.	Het systeem kan met nieuwe lidstaten worden uitgebreid.
48.	De applicatie kan gemakkelijk worden geïnstalleerd door personeel met een minimum aan IT-kwalificaties en -ervaring. De installatieprocedure moet zoveel mogelijk worden geautomatiseerd.
49.	Het systeem voorziet in een permanente test- en acceptatieomgeving.
50.	De jaarlijkse onderhouds- en ondersteuningskosten zijn zo laag mogelijk gehouden, doordat marktnormen zijn overgenomen en de applicatie zodanig is uitgewerkt dat zo weinig mogelijk ondersteuning van een centrale service desk vereist is.

3.2.8. Ontwerpeisen

Nr.	Beschrijving
51.	Het systeem is ontworpen en gedocumenteerd voor een operationele levensduur van ettelijke jaren.
52.	Het systeem is zodanig ontworpen dat het onafhankelijk is van de netwerkleverancier.
53.	Het systeem voldoet aan de bestaande apparatuur en programmatuur in de lidstaten, doordat het door middel van een op open normen gebaseerde web service technologie (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 enz.) met de registratiesystemen van de lidstaten interageert.

3.2.9. Geldende normen

Nr.	Beschrijving
54.	Het systeem voldoet aan de gegevensbeschermingsvoorschriften van Verordening (EG) nr. 45/2001 (artikelen 21, 22 en 23) en Richtlijn 95/46/EG.
55.	Het systeem voldoet aan de IDA-normen.
56.	Het systeem ondersteunt UTF8.

HOOFDSTUK 4: **Evaluatie**

1. ***Evaluatieprocedure overeenkomstig artikel 20 (uitwerking van besluiten overeenkomstig artikel 25, lid 2, van Besluit 2008/615/JBZ)***

1.1. *Vragenlijst*

De betrokken Raadsgroep zal een vragenlijst opstellen voor elke vorm van geautomatiseerde uitwisseling van gegevens bedoeld in hoofdstuk 2 van Besluit 2008/615/JBZ.

Zodra een lidstaat van oordeel is dat hij aan de voorwaarden voor het uitwisselen van gegevens in een bepaalde gegevenscategorie voldoet, beantwoordt hij de desbetreffende vragenlijst.

1.2. *Proefproject*

Met het oog op de evaluatie van de antwoorden op de vragenlijst voert de lidstaat die een aanvang wenst te maken met het uitwisselen van gegevens een proefproject uit met een of meer andere lidstaten die reeds gegevens uitwisselen uit hoofde van het Raadsbesluit. Het proefproject vindt plaats kort voor of kort na het evaluatiebezoek.

De voorwaarden en praktische regelingen van dit proefproject zullen door de betrokken Raadsgroep worden vastgesteld en worden gebaseerd op een individuele overeenkomst die voordien met de betrokken lidstaat is gesloten. De lidstaten die aan het proefproject deelnemen, bepalen zelf de praktische details van het project.

1.3. *Evaluatiebezoek*

Met het oog op de evaluatie van de antwoorden op de vragenlijst vindt een evaluatiebezoek plaats in de lidstaat die een aanvang wenst te maken met het uitwisselen van gegevens.

De voorwaarden en praktische regeling van dit bezoek zullen door de betrokken Raadsgroep worden vastgesteld en worden vooraf gebaseerd op een individuele overeenkomst tussen de betrokken lidstaat en het evaluatieteam. De betrokken lidstaat staat toe dat het evaluatieteam de geautomatiseerde uitwisseling van gegevens voor de te evalueren categorie(ën) controleert, met name door een programma voor het bezoek te organiseren dat rekening houdt met de verzoeken van het evaluatieteam.

Het evaluatieteam stelt binnen de maand een verslag van zijn evaluatiebezoek op en zendt dat toe aan de betrokken lidstaat, met het verzoek eventuele opmerkingen kenbaar te maken. Het evaluatieteam zal zijn verslag zo nodig herzien op basis van de opmerkingen van de lidstaat.

Het evaluatieteam bestaat uit ten hoogste 3 deskundigen, aangewezen door de lidstaten die deelnemen aan de geautomatiseerde uitwisseling voor de te evalueren gegevenscategorieën; deze deskundigen moeten ervaring hebben op het gebied van de betrokken gegevenscategorie, beschikken over een passende nationale veiligheidsmachtiging voor dergelijke aangelegenheden en bereid zijn aan ten minste één evaluatiebezoek in een andere lidstaat deel te nemen. De Commissie zal als waarnemer in het evaluatieteam worden uitgenodigd.

De leden van het evaluatieteam eerbiedigen de vertrouwelijke aard van de informatie waarvan zij in de uitvoering van hun taak kennis krijgen.

1.4. *Verslag aan de Raad*

Met het oog op het besluit bedoeld in artikel 25, lid 2, van Besluit 2008/615/JBZ zal aan de Raad een algemeen evaluatieverslag worden voorgelegd waarin de antwoorden op de vragenlijsten en de resultaten van het evaluatiebezoek en het proefproject worden gebundeld.

2. ***Evaluatieprocedure overeenkomstig artikel 21***

2.1. *Statistieken en rapportering*

Elke lidstaat stelt statistieken op over de resultaten van de geautomatiseerde gegevensuitwisseling. De betrokken Raadsgroep zal een model voor deze statistieken uitwerken, zodat deze kunnen worden vergeleken.

Deze statistieken worden jaarlijks toegezonden aan het secretariaat-generaal, dat een overzicht voor het voorbije jaar opstelt, en aan de Commissie.

Daarnaast zal de lidstaten op gezette tijden, maar niet meer dan één keer per jaar, worden verzocht andere informatie te verstrekken over de administratieve, technische en financiële implementatie van de geautomatiseerde gegevensuitwisseling die nodig is om het proces te analyseren en te verbeteren. Op basis daarvan zal een verslag aan de Raad worden opgesteld.

2.2. *Herziening*

De Raad zal binnen een redelijk tijdsbestek bovenbedoeld evaluatiemechanisme beoordelen en zo nodig herzien.

3. Vergaderingen van deskundigen

De deskundigen komen regelmatig bijeen in de betrokken Raadsgroep om bovenbedoelde evaluatieprocedures te organiseren en te implementeren, alsook om ervaringen uit te wisselen en mogelijke verbeteringen te bespreken. De resultaten van deze besprekingen op deskundigenniveau zullen, voor zover van toepassing, in het verslag bedoeld in punt 2.1 worden opgenomen.

BESLUIT 2008/617/JBZ VAN DE RAAD

van 23 juni 2008

ter verbetering van de samenwerking in crisissituaties tussen de speciale interventie-eenheden van de lidstaten van de Europese Unie

DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag betreffende de Europese Unie, met name op artikel 30, artikel 32 en artikel 34, lid 2, onder c),

Gezien het initiatief van de Republiek Oostenrijk ([1]),

Gezien het advies van het Europees Parlement ([2]),

Overwegende hetgeen volgt:

(1) Volgens artikel 29 van het Verdrag is het doel van de Unie de burgers in een ruimte van vrijheid, veiligheid en rechtvaardigheid een hoog niveau van zekerheid te verschaffen door de ontwikkeling van een gezamenlijk optreden van de lidstaten op het gebied van politiële en justitiële samenwerking in strafzaken.

(2) De staatshoofden en regeringsleiders van de lidstaten van de Europese Unie hebben in hun op 25 maart 2004 afgelegde Verklaring inzake solidariteit tegenover terrorisme het vaste voornemen uitgesproken dat de lidstaten alle tot hun beschikking staande middelen zullen inzetten om, in geval van een terroristische aanval, op verzoek van de politieke autoriteiten van een lidstaat of een toetredend land bijstand te verlenen op het grondgebied van die lidstaat of dat land.

(3) Na de aanslagen van 11 september 2001 hebben de speciale interventie-eenheden van alle rechtshandhavingsinstanties van de lidstaten onder auspiciën van de Task Force Hoofden van Politie reeds een begin gemaakt met bepaalde vormen van samenwerking. In het kader van dit netwerk, „Atlas" genaamd, hebben sinds 2001 verschillende studiebijeenkomsten en gezamenlijke oefeningen plaatsgevonden, zijn studies uitgevoerd en is materiaal uitgewisseld.

(4) Geen enkele lidstaat beschikt over alle middelen en deskundigheid om het hoofd te bieden aan alle soorten specifieke of grootschalige crisissituaties die een speciale interventie vergen. De mogelijkheid om een andere lidstaat om bijstand te verzoeken is dan ook van cruciaal belang.

(5) In Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit ([3]) (het „besluit van Prüm"), en met name in artikel 18 daarvan, worden regels vastgesteld voor vormen van politiële bijstand tussen de lidstaten in verband met massabijeenkomsten en soortgelijke grootschalige evenementen, rampen en zware ongevallen. Dit besluit heeft geen betrekking op massabijeenkomsten, natuurrampen of zware ongevallen in de zin van artikel 18 van het besluit van Prüm, maar vormt een aanvulling op de bepalingen van het besluit van Prüm die betrekking hebben op vormen van politiële bijstand tussen de speciale interventie-eenheden van de lidstaten in andere situaties, namelijk in door mensen veroorzaakte crisissituaties die een ernstig rechtstreeks fysiek of materieel risico inhouden voor personen, eigendom, infrastructuur of instanties, waarbij met name moet worden gedacht aan gijzelingen, kapingen en soortgelijke gebeurtenissen.

(6) Met dit juridische kader en de lijst van de bevoegde instanties zullen de lidstaten in staat zijn snel te reageren en tijd te winnen in geval van dergelijke crisissituaties. Teneinde de lidstaten beter in staat te stellen dergelijke crisissituaties, en met name terroristische incidenten, te voorkomen en erop te reageren, is het bovendien van essentieel belang dat de speciale interventie-eenheden regelmatig bijeenkomen en gezamenlijke opleidingen organiseren, zodat zij profijt kunnen trekken van elkaars ervaringen,

BESLUIT:

Artikel 1

Onderwerp

In dit besluit worden de algemene voorschriften en voorwaarden vastgesteld voor bijstandverlening door en/of een optreden van de speciale interventie-eenheden van een lidstaat op het grondgebied van een andere lidstaat (hierna „verzoekende lidstaat" genoemd) wanneer deze eenheden hierom door de verzoekende lidstaat is verzocht, en zij op dit verzoek zijn ingegaan teneinde het hoofd te bieden aan een crisissituatie. De praktische gegevens en de uitvoeringsregelingen waarmee dit besluit wordt aangevuld, worden rechtstreeks overeengekomen tussen de verzoekende lidstaat en de aangezochte lidstaat.

Artikel 2

Definities

In dit besluit wordt verstaan onder:

a) „speciale interventie-eenheid": een rechtshandhavingseenheid van een lidstaat die gespecialiseerd is in crisisbeheersing;

([1]) PB C 321 van 29.12.2006, blz. 45.

([2]) Advies van 31 januari 2008 (nog niet bekendgemaakt in het Publicatieblad).

([3]) Zie bladzijde 1 van dit Publicatieblad.

b) „crisissituatie": een situatie waarin de bevoegde instanties van een lidstaat op redelijke gronden kunnen aannemen dat er sprake is van een strafbaar feit dat een ernstige rechtstreekse fysieke of materiële bedreiging vormt voor personen, eigendom, infrastructuur of instanties in die lidstaat, met name situaties als bedoeld in artikel 1, lid 1, van Kaderbesluit 2002/475/JBZ van 13 juni 2006 inzake terrorismebestrijding ([1]);

c) „bevoegde instantie": de nationale instantie die verzoeken doet uitgaan en toestemming verleent voor het inzetten van de speciale interventie-eenheden.

Artikel 3

Bijstand aan een andere lidstaat

1. Door middel van een verzoek via de bevoegde instanties, dat een toelichting bevat met betrekking tot de aard van de gewenste bijstand en de operationele noodzaak ervan, kan een lidstaat vragen om bijstand door een speciale interventie-eenheid van een andere lidstaat voor het aanpakken van een crisissituatie. De bevoegde instantie van de aangezochte lidstaat kan een dergelijk verzoek aanvaarden of weigeren, of andere dan de gevraagde bijstand voorstellen.

2. Bijstand kan, onder voorbehoud van een akkoord tussen de betrokken lidstaten, bestaan in het verstrekken van uitrusting en/of deskundigheid aan de verzoekende lidstaat, en/of het uitvoeren van acties op het grondgebied van die lidstaat, zo nodig met gebruikmaking van wapens.

3. In het geval van acties op het grondgebied van de verzoekende lidstaat worden functionarissen van de bijstandverlenende speciale interventie-eenheid gemachtigd om op het grondgebied van de verzoekende lidstaat in een ondersteunende functie op te treden en alle nodige maatregelen te nemen om de verzochte bijstand te verlenen; daarbij

a) treden deze functionarissen op onder de verantwoordelijkheid, het gezag en de leiding van de verzoekende lidstaat, overeenkomstig het recht van de verzoekende lidstaat, en tevens

b) treden deze functionarissen op binnen de grenzen van de bevoegdheden die hun krachtens hun eigen nationale wetgeving zijn toegekend.

Artikel 4

Wettelijke en strafrechtelijke aansprakelijkheid

Wanneer functionarissen van een lidstaat in een andere lidstaat optreden en/of uitrusting gebruikt wordt in het kader van dit besluit, zijn de bepalingen inzake wettelijke en strafrechtelijke aansprakelijkheid van de artikelen 21, leden 4 en 5, en artikel 22 van het besluit van Prüm van toepassing.

([1]) PB L 164 van 22.6.2002, blz. 3.

Artikel 5

Bijeenkomsten en gezamenlijke opleidingen

De deelnemende lidstaten zien erop toe dat hun speciale interventie-eenheden zo nodig bijeenkomsten beleggen en gezamenlijke opleidingen en oefeningen organiseren teneinde ervaring en deskundigheid alsook algemene, praktische en technische informatie uit te wisselen over het aanpakken van crisissituaties. Deze bijeenkomsten, opleidingen en oefeningen kunnen worden gefinancierd in het kader van de mogelijkheden die de financiële programma's van de Unie bieden om subsidies uit de begroting van de Europese Unie te verwerven. De lidstaat die het voorzitterschap van de Unie bekleedt, zal er in dit verband voor trachten te zorgen dat deze bijeenkomsten, opleidingen en oefeningen daadwerkelijk plaatsvinden.

Artikel 6

Kosten

De verzoekende lidstaat draagt de operationele kosten van de speciale interventie-eenheden van de aangezochte lidstaat in verband met de toepassing van artikel 3, met inbegrip van de kosten van vervoer en huisvesting, tenzij tussen de betrokken lidstaten anders wordt overeengekomen.

Artikel 7

Verhouding tot andere instrumenten

1. Onverminderd hun verbintenissen uit hoofde van andere wetgevingsbesluiten die ingevolge titel VI van het Verdrag zijn aangenomen, met name het besluit van Prüm:

a) staat het de lidstaten vrij om bilaterale of multilaterale overeenkomsten of regelingen betreffende grensoverschrijdende samenwerking die van kracht zijn op 23 juni 2008, te blijven toepassen, voor zover deze overeenkomsten of regelingen niet onverenigbaar zijn met de doelstellingen van dit besluit.

b) staat het de lidstaten vrij om bilaterale of multilaterale overeenkomsten of regelingen betreffende grensoverschrijdende samenwerking aan te gaan of in werking te doen treden na 23 december 2008, voor zover deze overeenkomsten of regelingen de mogelijkheid bieden de doelstellingen van dit besluit tussen de lidstaten te verruimen of te verbreden.

2. De in lid 1 bedoelde overeenkomsten en regelingen laten de betrekkingen met de lidstaten die daarbij geen partij zijn, onverlet.

3. De lidstaten stellen de Raad en de Commissie in kennis van de in lid 1 bedoelde overeenkomsten en regelingen.

Artikel 8

Slotbepalingen

Het secretariaat-generaal van de Raad stelt een lijst op van de bevoegde instanties van de lidstaten die verzoeken kunnen indienen en toestemming mogen geven voor de verlening van de in artikel 3 bedoelde bijstand, en werkt deze lijst bij.

Het secretariaat-generaal van de Raad stelt de in de eerste alinea bedoelde instanties op de hoogte van alle wijzigingen in de uit hoofde van dit artikel opgestelde lijst.

Artikel 9

Inwerkingtreding

Dit besluit treedt in werking op 23 december 2008.

Gedaan te Luxemburg, 23 juni 2008.

Voor de Raad

De voorzitter

I. JARC