ISSN 1725-2628

Europeiska unionens officiella tidning

L 210

femtioförsta årgången

6 augusti 2008

Svensk utgåva

Lagstiftning

Innehållsförteckning

III *Rättsakter som antagits i enlighet med fördraget om Europeiska unionen*

RÄTTSAKTER SOM ANTAGITS I ENLIGHET MED AVDELNING VI I FÖRDRAGET OM EUROPEISKA UNIONEN

⋆ **Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet** 1

⋆ **Rådets beslut 2008/616/RIF av den 23 juni 2008 om genomförande av beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet** 12

⋆ **Rådets beslut 2008/617/RIF av den 23 juni 2008 om förbättrat samarbete i krissituationer mellan Europeiska unionens medlemsstaters särskilda insatsgrupper** 73

Pris: 18 EUR

SV

De rättsakter vilkas titlar är tryckta med fin stil är sådana rättsakter som har avseende på den löpande handläggningen av jordbrukspolitiska frågor. De har normalt en begränsad giltighetstid.

Beträffande alla övriga rättsakter gäller att titlarna är tryckta med fetstil och föregås av en asterisk.

III

(Rättsakter som antagits i enlighet med fördraget om Europeiska unionen)

RÄTTSAKTER SOM ANTAGITS I ENLIGHET MED AVDELNING VI I FÖRDRAGET OM EUROPEISKA UNIONEN

RÅDETS BESLUT 2008/615/RIF

av den 23 juni 2008

om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet

EUROPEISKA UNIONENS RÅD HAR BESLUTAT FÖLJANDE

med beaktande av fördraget om Europeiska unionen, särskilt artikel 30.1 a och b, artikel 31.1 a, artikel 32 och artikel 34.2 c,

på initiativ av Konungariket Belgien, Republiken Bulgarien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Republiken Italien, Storhertigdömet Luxemburg, Konungariket Nederländerna, Republiken Österrike, Republiken Portugal, Rumänien, Republiken Slovenien, Republiken Slovakien, Republiken Finland och Konungariket Sverige,

med beaktande av Europaparlamentets yttrande ([1]), och

av följande skäl:

(1) Efter ikraftträdandet av fördraget mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (Prümfördraget) läggs, i enlighet med bestämmelserna i fördraget om Europeiska unionen efter samråd med Europeiska kommissionen, detta initiativ fram i syfte att införliva innebörden av bestämmelserna i Prümfördraget med Europeiska unionens lagstiftning.

(2) I slutsatserna från Europeiska rådets möte i Tammerfors i oktober 1999 bekräftades behovet av förbättrat informationsutbyte mellan medlemsstaternas behöriga myndigheter för att upptäcka och utreda brott.

(3) I Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen från november 2004 ger Europeiska rådet uttryck för sin övertygelse om att det för detta syfte krävs en innovativ strategi i fråga om gränsöverskridande utbyte av information om brottsbekämpning.

(4) Europeiska rådet angav i enlighet med detta att utbytet av sådan information bör uppfylla de villkor som gäller för tillgänglighetsprincipen. Detta innebär att en brottsbekämpande tjänsteman i en av unionens medlemsstater som behöver information för att utföra sina uppgifter kan få denna från en annan medlemsstat och att de brottsbekämpande myndigheterna i den medlemsstat som innehar denna information kommer att göra den tillgänglig för det angivna ändamålet, med hänsyn tagen till behov med anknytning till pågående utredningar i den medlemsstaten.

(5) Europeiska rådet fastställde den 1 januari 2008 som tidsfrist för att uppnå detta mål i Haagprogrammet.

(6) Redan i rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater ([2]) fastställs regler enligt vilka medlemsstaternas brottsbekämpande myndigheter effektivt och snabbt kan utbyta befintlig information och befintliga underrättelser för genomförandet av brottsutredningar eller kriminalunderrättelseverksamhet.

(7) I Haagprogrammet för stärkt frihet, säkerhet och rättvisa förklaras också att ny teknik bör användas fullt ut och att det också bör finnas ömsesidig tillgång till nationella databaser, men att nya centraliserade europeiska databaser bör inrättas endast på grundval av studier som har visat deras mervärde.

([1]) Yttrandet avgivet den 10 juni 2007 (ännu ej offentliggjort i EUT).

([2]) EUT L 386, 29.12.2006, s. 89.

(8) För ett effektivt internationellt samarbete är det av central betydelse att exakt information kan utbytas snabbt och effektivt. Syftet är att införa förfaranden för att främja ett snabbt, effektivt och billigt utbyte av uppgifter. För den gemensamma användningen av uppgifter bör ansvarsskyldighet gälla för dessa förfaranden, och de bör innehålla lämpliga garantier beträffande uppgifternas korrekthet och säkerhet under överföring och lagring samt förfaranden för registrering av utbyte av uppgifter och restriktioner beträffande användningen av utbytta uppgifter.

(9) Dessa krav uppfylls genom Prümfördraget. För att de väsentliga kraven i Haagprogrammet ska kunna uppfyllas för samtliga medlemsstater inom den tidsram som fastställs där bör innebörden av de väsentliga delarna av Prümfördraget göras tillämpliga på samtliga medlemsstater.

(10) Detta beslut innehåller därför bestämmelser som är grundade på de viktigaste bestämmelserna i Prümfördraget och som är avsedda att förbättra informationsutbytet, varigenom medlemsstaterna beviljar varandra rätt till tillgång till sina automatiska databaser över DNA-analyser, automatiska identifieringssystem för fingeravtryck och uppgifter i fordonsregister. När det gäller uppgifter från nationella databaser över DNA-analyser och automatiska identifieringssystem för fingeravtryck bör det genom ett system med träff/icke träff vara möjligt för den medlemsstat som genomför sökningen att i ett andra steg begära specifika personuppgifter från den medlemsstat som administrerar uppgifterna och vid behov begära ytterligare uppgifter genom förfaranden för ömsesidigt bistånd, inklusive de förfaranden som har antagits enligt rambeslut 2006/960/RIF.

(11) Detta skulle påskynda de befintliga förfarandena avsevärt genom att det blir möjligt för medlemsstaterna att ta reda på om någon annan medlemsstat, och i så fall vilken, har de uppgifter som de behöver.

(12) Gränsöverskridande jämförelse av uppgifter bör öppna en ny dimension inom brottsbekämpningen. Den information som erhålls genom jämförelse av uppgifter bör öppna vägen för nya utredningsstrategier för medlemsstaterna och alltså spela en central roll när det gäller att bistå medlemsstaternas brottsbekämpande och rättsliga myndigheter.

(13) Reglerna bygger på inrättande av nätverk mellan medlemsstaternas nationella databaser.

(14) På vissa villkor bör medlemsstaterna kunna översända personuppgifter och icke-personuppgifter för att förbättra informationsutbytet för att förebygga brott och upprätthålla den allmänna ordningen och säkerheten i samband med större evenemang med gränsöverskridande verkningar.

(15) Vid tillämpningen av artikel 12 får medlemsstaterna besluta att prioritera kampen mot allvarlig brottslighet med beaktande av de begränsade tekniska resurser som finns tillgängliga för överföringen av uppgifter.

(16) Förutom förbättring av informationsutbytet finns det behov av en reglering av andra former för närmare samarbete mellan polismyndigheterna, särskilt vid gemensamma säkerhetsoperationer (t.ex. gemensamma patruller).

(17) Närmare polissamarbete och straffrättsligt samarbete måste gå hand i hand med respekt för grundläggande rättigheter, särskilt rätten till respekt för integritet och till skydd av personuppgifter, som bör garanteras genom särskilda förfaranden för uppgiftsskydd som är särskilt anpassade till den specifika arten av olika former av uppgiftsutbyte. Sådana bestämmelser om uppgiftsskydd bör särskilt beakta särdragen i gränsöverskridande elektronisk åtkomst till databaser. Eftersom det med åtkomst on-line inte är möjligt för den medlemsstat som administrerar uppgifterna att göra kontroller i förväg bör ett system för kontroll i efterhand finnas.

(18) Systemet med träff/icke-träff tillhandahåller en struktur med jämförelse av anonyma profiler, där ytterligare personuppgifter endast utbyts efter en träff, för vilket tillgången och mottagandet styrs av nationell lagstiftning, inbegripet regler om rättsligt bistånd. Denna konstruktion garanterar systemet med träff/icke-träff tillfredsställande skydd av personuppgifter, varvid dock översändandet av personuppgifter till en annan medlemsstat förutsätter tillräcklig dataskyddsnivå i den mottagande medlemsstaten.

(19) Med tanke på det omfattande utbyte av information och uppgifter som följer av närmare polisiärt och rättsligt samarbete eftersträvar man med detta beslut att garantera en lämplig nivå av uppgiftsskydd. Det följer den skyddsnivå som utformats för databehandling i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter, tilläggsprotokollet till konventionen av den 8 november 2001 och principerna i Europarådets rekommendation nr R (87) 15 om polisens användning av personuppgifter.

(20) Bestämmelserna om dataskydd i detta beslut inbegriper även de dataskyddsprinciper som var nödvändiga på grund av avsaknaden av ett rambeslut om dataskydd i den tredje pelaren. Detta rambeslut bör tillämpas inom hela området för polissamarbete och straffrättsligt samarbete under förutsättning att dess dataskyddsnivå inte är lägre än det skydd som fastställs i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter och i dess tilläggsprotokoll av den 8 november 2001 samt att Europarådets ministerkommittés rekommendation R (87) 15 av den 17 september 1987 om polisens användning av personuppgifter beaktas, även när uppgifter inte behandlas automatiskt.

(21) Eftersom målen för detta beslut, särskilt förbättrandet av informationsutbytet i Europeiska unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna själva på grund av brottsbekämpningens och säkerhetsfrågornas gränsöverskridande natur, vilket innebär att medlemsstaterna är ömsesidigt beroende av varandra i dessa frågor, och de därför bättre kan uppnås på EU-nivå, kan rådet vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om upprättandet av Europeiska gemenskapen, till vilken artikel 2 i fördraget om Europeiska unionen hänvisar. I enlighet med proportionalitetsprincipen i artikel 5 i EG-fördraget går detta beslut inte utöver vad som är nödvändigt för att uppnå dessa mål.

(22) Detta beslut står i överensstämmelse med de grundläggande rättigheter och principer som erkänns särskilt i Europeiska unionens stadga om de grundläggande rättigheterna.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA ASPEKTER

Artikel 1

Syfte och tillämpningsområde

Genom detta beslut har medlemsstaterna för avsikt att fördjupa det gränsöverskridande samarbetet i frågor som omfattas av avdelning VI i fördraget, särskilt i fråga om utbyte av information mellan myndigheter som är ansvariga för förebyggande och utredning av brott. Beslutet innehåller därför regler på följande områden:

a) Bestämmelser om villkoren och förfarandet för automatisk överföring av DNA-profiler, fingeravtrycksuppgifter och vissa uppgifter ur nationella fordonsregister (kapitel 2).

b) Bestämmelser om villkoren för översändande av uppgifter i samband med större evenemang med gränsöverskridande verkningar (kapitel 3).

c) Bestämmelser om villkoren för översändande av uppgifter för förebyggande av terroristbrott (kapitel 4).

d) Bestämmelser om villkoren och förfarandet för fördjupat gränsöverskridande polissamarbete genom olika åtgärder (kapitel 5).

KAPITEL 2

ÅTKOMST ON-LINE OCH BEGÄRAN OM UPPFÖLJNING

AVSNITT 1

DNA-profiler

Artikel 2

Inrättande av nationella databaser med DNA-analyser

1. Medlemsstaterna ska inrätta och upprätthålla nationella databaser med DNA-analyser för brottsutredningar. Behandlingen av uppgifter i dessa databaser inom ramen för detta beslut ska utföras i enlighet med detta beslut, i överensstämmelse med nationell rätt som är tillämplig på behandlingen.

2. För genomförandet av detta beslut ska medlemsstaterna se till att det i överensstämmelse med punkt 1 första meningen bereds tillgång till referensuppgifterna i de nationella databaserna med DNA-analyser. Referensuppgifterna ska endast innehålla DNA-profiler från den icke-kodifierande delen av DNA:t och en sifferbeteckning. Referensuppgifterna får inte innehålla uppgifter som möjliggör en omedelbar identifiering av den berörda personen. Referensuppgifter, som inte är kopplade till en viss person (oidentifierade DNA-profiler), ska kunna identifieras som sådana.

3. Varje medlemsstat ska underrätta rådets generalsekretariat om de nationella databaser med DNA-analyser på vilka artiklarna 2–6 kan tillämpas samt villkoren förutsättningarna för automatisk sökning som avses i artikel 3.1 i enlighet med artikel 36.

Artikel 3

Automatisk sökning av DNA-profiler

1. I samband med brottsutredningar ska medlemsstaterna ge de övriga medlemsstaternas nationella kontaktställen enligt artikel 6 tillträde till referensuppgifterna i sina databaser med DNA-profiler med rätt att göra automatiska sökningar i dem genom jämförelse av DNA-profiler. Sökningen får endast göras i enskilda fall och i överensstämmelse med den nationella lagstiftningen i den ansökande medlemsstaten.

2. Om det i samband med en automatisk sökning konstateras att en förmedlad DNA-profil motsvarar DNA-profiler i den mottagande medlemsstatens databas, ska det nationella kontaktstället i den ansökande medlemsstaten automatiskt ta emot de referensuppgifter för vilka överensstämmelse har konstaterats. Om ingen överensstämmelse konstateras ska detta meddelas automatiskt.

Artikel 4

Automatisk jämförelse av DNA-profiler

1. Medlemsstaterna ska i samband med brottsutredningar enligt en gemensam överenskommelse genom sina nationella kontaktställen jämföra DNA-profilerna för sina egna oidentifierade DNA-profiler med referensuppgifterna för alla övriga parters nationella databaser med DNA-analyser. Profilerna ska översändas och jämföras automatiskt. Oidentifierade DNA-profiler ska översändas för jämförelse endast i sådana fall där den ansökande medlemsstatens nationella lagstiftning tillåter det.

2. Om en medlemsstat till följd av en jämförelse enligt punkt 1 konstaterar att en översänd DNA-profil motsvarar en profil som ingår i någon av dess egna databaser med DNA-profiler ska den utan dröjsmål tillställa den andra medlemsstatens nationella kontaktställe de referensuppgifter för vilka överensstämmelse har konstaterats.

Artikel 5

Översändande av övriga personuppgifter och ytterligare information

Om en överensstämmelse mellan DNA-profiler konstateras vid förfaranden enligt artiklarna 3 och 4 ska översändande av övriga tillgängliga personuppgifter och ytterligare information med anknytning till referensuppgifterna regleras av den anmodade medlemsstatens nationella lagstiftning, inklusive bestämmelserna om rättshjälp.

Artikel 6

Nationellt kontaktställe och genomförandeåtgärder

1. Varje medlemsstat ska utse ett nationellt kontaktställe för förmedling av de uppgifter som avses i artiklarna 3 och 4. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

2. De tekniska detaljerna för det förfarande som beskrivs i artiklarna 3 och 4 ska fastställas i de genomförandeåtgärder som avses i artikel 33.

Artikel 7

Insamling av molekylärgenetiskt material och översändande av DNA-profiler

Om det under pågående brottsutredning eller straffrättsliga förfaranden saknas en DNA-profil över en viss person som vistas i en anmodad medlemsstat, ska den medlemsstaten ge rättshjälp genom att insamla och undersöka molekylärgenetiskt material från denna person och översända den DNA-profil som erhållits, om

a) den ansökande medlemsstaten meddelar för vilket ändamål detta behövs,

b) den ansökande medlemsstaten i enlighet med sin lagstiftning framställer en begäran eller ett förordnande om undersökning från den behöriga myndigheten, där det framgår att det hade funnits förutsättningar för insamling och undersökning av molekylärgenetiskt material om personen i fråga hade vistats i den ansökande medlemsstaten, och

c) det enligt lagstiftningen i den anmodade medlemsstaten finns förutsättningar för insamling och undersökning av molekylärgenetiskt material samt för översändande av den DNA-profil som erhålls.

AVSNITT 2

Fingeravtrycksuppgifter

Artikel 8

Fingeravtrycksuppgifter

För genomförandet av detta beslut ska medlemsstaterna se till att referensuppgifterna i de för brottsförebyggande och brottsutredning inrättade nationella systemen för automatisk identifiering av fingeravtryck hålls tillgängliga. Referensuppgifterna ska endast innehålla fingeravtrycksuppgifter och en sifferbeteckning. Referensuppgifterna får inte innehålla uppgifter som möjliggör en omedelbar identifiering av den berörda personen. Referensuppgifter som inte är kopplade till en viss person (”oidentifierade fingeravtrycksuppgifter”) ska kunna identifieras som sådana.

Artikel 9

Automatisk sökning av fingeravtrycksuppgifter

1. För förebyggande och utredning av brott ska medlemsstaterna ge de övriga medlemsstaternas nationella kontaktställen enligt artikel 11 tillträde till referensuppgifterna i de system för automatisk identifiering av fingeravtryck som inrättats för detta syfte och ska ge dem rätt att göra automatiska sökningar i dem genom jämförelse av fingeravtrycksuppgifter. Sökningen får endast göras i enskilda fall och i överensstämmelse med den nationella lagstiftningen i den ansökande medlemsstaten.

2. Bekräftelse av fingeravtrycksuppgifters överensstämmelse med referensuppgifterna hos den medlemsstat som administrerar databasen ska utföras av det nationella kontaktstället i den ansökande medlemsstaten genom att de referensuppgifter som krävs för att säkerställa en entydig överensstämmelse översänds automatiskt.

Artikel 10

Översändande av övriga personuppgifter och ytterligare information

Om en överensstämmelse mellan fingeravtrycksuppgifter konstateras vid ett förfarande enligt artikel 9 ska översändandet av övriga personuppgifter och ytterligare information med anknytning till referensuppgifterna regleras av den anmodade medlemsstatens nationella lagstiftning, inklusive bestämmelserna om rättslig hjälp.

Artikel 11

Nationellt kontaktställe och genomförandeåtgärder

1. Varje medlemsstat ska utse ett nationellt kontaktställe för förmedling av de uppgifter som avses i artikel 9. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

2. De tekniska detaljerna för det förfarande som anges i artikel 9 ska fastställas i de genomförandeåtgärder som avses i artikel 33.

AVSNITT 3

Uppgifter ur fordonsregister

Artikel 12

Automatisk sökning av uppgifter ur fordonsregister

1. För förebyggande och utredning av brott samt för undersökning av sådana överträdelser som i den ansökande medlemsstaten lyder under domstols- och åklagarväsendets behörighet samt för upprätthållande av allmän säkerhet ska medlemsstaterna ge övriga medlemsstaters nationella kontaktställen enligt punkt 2 tillträde till följande uppgifter i de nationella fordonsregistren, med rätt att i enskilda fall göra automatiska sökningar:

a) Uppgifter om ägare och innehavare.

b) Uppgifter om fordonet.

En sökning får endast genomföras genom användning av ett fordons fullständiga chassinummer eller fullständiga registreringsnummer. Sökningar får endast göras i överensstämmelse med den ansökande medlemsstatens nationella lagstiftning.

2. Varje medlemsstat ska för förmedling av de uppgifter som avses i punkt 1 utse ett nationellt kontaktställe som tar emot förfrågningar. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen. De tekniska detaljerna för förfarandet ska fastställas i de genomförandeåtgärder som avses i artikel 33.

KAPITEL 3

STÖRRE EVENEMANG

Artikel 13

Översändande av andra uppgifter än personuppgifter

För förebyggande av brott och upprätthållande av allmän ordning och säkerhet i samband med större evenemang med gränsöverskridande verkningar, såsom betydande idrottsevenemang eller Europeiska rådets möten, ska medlemsstaterna både på begäran och på eget initiativ i överensstämmelse med den översändande medlemsstatens nationella lagstiftning sända varandra nödvändiga icke personrelaterade uppgifter.

Artikel 14

Översändande av personuppgifter

1. För förebyggande bekämpning av brott och upprätthållande av allmän ordning och säkerhet i samband med större evenemang med gränsöverskridande verkningar, såsom betydande idrottsevenemang eller Europeiska rådets möten, ska medlemsstaterna både på begäran och på eget initiativ sända varandra personuppgifter, om det på grundval av domar som vunnit laga kraft eller andra fakta finns skäl att anta att personerna i fråga kommer att begå brott vid de berörda evenemangen eller att personerna utgör ett hot mot den allmänna ordningen och säkerheten, förutsatt att översändande av sådana uppgifter är tillåtet enligt den nationella lagstiftningen i den medlemsstat som sänder uppgifterna.

2. Personuppgifter får endast behandlas för de syften som avses i punkt 1 och endast i samband med de evenemang för vilket de har översänts. De uppgifter som har översänts ska utplånas omedelbart när de syften som avses i punkt 1 har uppnåtts eller när de inte längre kan uppnås. De uppgifter som översänts ska under alla omständigheter utplånas senast inom ett år.

Artikel 15

Nationellt kontaktställe

Varje medlemsstat ska utse ett nationellt kontaktställe för förmedling av de uppgifter som avses i artiklarna 13 och 14. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

KAPITEL 4

ÅTGÄRDER FÖR FÖREBYGGANDE AV TERRORISTBROTT

Artikel 16

Översändande av uppgifter för bekämpning av terroristbrott

1. Medlemsstaterna får i överensstämmelse med nationell lagstiftning och i enskilda fall, även utan föregående förfrågan, för förebyggande av terroristbrott översända personuppgifter och andra uppgifter enligt punkt 2 till de övriga medlemsstaternas nationella kontaktställen enligt punkt 3, i den mån det är nödvändigt därför att särskilda omständigheter ger anledning att anta att de berörda personerna kommer att göra sig skyldiga till sådana brott som avses i artiklarna 1–3 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism ([1]).

([1]) EGT L 164, 22.6.2002, s. 3.

2. De uppgifter som ska översändas är efternamn, förnamn, födelsetid och födelseort samt en beskrivning av de omständigheter som ligger till grund för det antagande som avses i punkt 1.

3. Varje medlemsstat ska utse ett nationellt kontaktställe för utbyte av information med övriga medlemsstaters nationella kontaktställen. De nationella kontaktställenas befogenheter ska fastställas i enlighet med den tillämpliga nationella lagstiftningen.

4. Den översändande medlemsstaten kan i enlighet med den nationella lagstiftningen fastställa de villkor enligt vilka den mottagande medlemsstaten får använda sådana uppgifter. Dessa villkor ska vara bindande för den mottagande medlemsstaten.

KAPITEL 5

ANDRA FORMER AV SAMARBETE

Artikel 17

Gemensamma insatser

1. För att fördjupa polissamarbetet kan de behöriga myndigheter som medlemsstaterna utser, för upprätthållande av allmän ordning och säkerhet samt för förebyggande av brott, inrätta gemensamma patruller och genomföra andra gemensamma insatser där utsedda tjänstemän eller andra statsanställda (nedan kallade *tjänstemän*) från andra medlemsstater deltar i insatser på en annan medlemsstats territorium.

2. Varje medlemsstat får i egenskap av värdmedlemsstat, i enlighet med sin nationella lagstiftning och med den utsändande medlemsstatens medgivande, ge tjänstemän från de utsändande medlemsstaterna rätt att utöva verkställande befogenheter i samband med gemensamma insatser eller, när detta är tillåtet enligt värdmedlemsstatens lagstiftning, bevilja de utsändande medlemsstaternas tjänstemän rätt att utöva verkställande befogenheter i enlighet med den utsändande medlemsstatens lagstiftning. Sådana verkställande befogenheter får endast utövas under överinsyn av och i regel i närvaro av värdmedlemsstatens tjänstemän. De utsändande medlemsstaternas tjänstemän ska lyda under värdmedlemsstatens nationella lagstiftning. Värdmedlemsstaten ska ansvara för deras handlingar.

3. Tjänstemän från utsändande medlemsstater som deltar i gemensamma insatser ska iaktta de anvisningar som meddelas av värdmedlemsstatens behöriga myndighet.

4. Medlemsstaterna ska lämna förklaringar enligt artikel 36 i vilka de fastställer de praktiska aspekterna av samarbetet.

Artikel 18

Bistånd vid större evenemang, katastrofer och allvarliga olyckor

Medlemsstaternas behöriga myndigheter ska ge varandra ömsesidigt bistånd i enlighet med sin nationella lagstiftning vid större evenemang, och liknande viktiga händelser, katastrofer och allvarliga olyckor, genom att försöka förhindra brott och upprätthålla allmän ordning och säkerhet, genom att

a) i ett så tidigt skede som möjligt underrätta varandra om sådana situationer som har gränsöverskridande verkningar, och förmedla väsentliga uppgifter som hänför sig till dem,

b) i situationer med gränsöverskridande verkningar genomföra och samordna nödvändiga polisiära åtgärder på sitt territorium,

c) på begäran av den medlemsstat på vars territorium situationen i fråga har uppstått, i den mån det är möjligt, ge bistånd genom att sända tjänstemän, specialister och rådgivare samt genom att ställa övrig nödvändig utrustning till förfogande.

Artikel 19

Användning av tjänstevapen, ammunition och övrig nödvändig utrustning

1. En utsändande medlemsstats tjänstemän som inom ramen för en gemensam insats vistas på en annan medlemsstats territorium enigt artikel 17 eller 18 får använda sin nationella tjänsteuniform. De får inneha tjänstevapen, ammunition och övrig nödvändig utrustning i enlighet med den utsändande medlemsstatens nationella lagstiftning. Värdmedlemsstaten får förbjuda den utsändande medlemsstatens tjänstemän att medföra vissa tjänstevapen, viss ammunition eller utrustning.

2. Medlemsstaterna ska lämna förklaringar enligt artikel 36 i vilka de förtecknar de tjänstevapen, den ammunition och utrustning som endast får användas vid nödvärn för att skydda sig själv eller andra. Värdmedlemsstatens tjänsteman som leder insatsen kan i enskilda fall i enlighet med den nationella lagstiftningen godkänna användning av tjänstevapen, ammunition och utrustning i andra fall än de som avses i första meningen. Vid användning av tjänstevapen, ammunition och övrig nödvändig utrustning ska värdmedlemsstatens lagstiftning iakttas. De behöriga myndigheterna ska underrätta varandra om tillåtna tjänstevapen och tillåten ammunition och utrustning och villkoren för användningen av dem.

3. Om en medlemsstats tjänstemän i samband med åtgärder i enlighet med detta beslut använder motorfordon på en annan medlemsstats territorium, ska för dem gälla samma trafikbestämmelser som för värdmedlemsstatens tjänstemän, inklusive de bestämmelser om skyldighet att lämna företräde och särskilda rättigheter i vägtrafiken.

4. Medlemsstaterna ska lämna förklaringar enligt artikel 36 i vilka de fastställer de praktiska aspekterna i samband med användningen av tjänstevapen, ammunition och utrustning.

Artikel 20

Skydd och bistånd

Medlemsstaterna ska vara skyldiga att skydda och bistå andra medlemsstaters tjänstemän som överskrider gränserna på samma sätt som sina egna tjänstemän.

Artikel 21

Allmänna bestämmelser om skadeståndsansvar

1. När en medlemsstats tjänstemän verkar i en annan medlemsstat i enlighet med artikel 17, ska deras medlemsstat ansvara för de eventuella skador som de förorsakar under sina insatser, i enlighet med lagstiftningen i den medlemsstat på vars territorium de verkar.

2. Den medlemsstat på vars territorium de skador som avses i punkt 1 förorsakades ska ersätta sådana skador enligt de villkor som gäller för skador som förorsakas av dess egna tjänstemän.

3. I det fall som anges i punkt 1 ska den medlemsstat vars tjänstemän har förorsakat skador på någon person på en annan medlemsstats territorium till fullo ersätta den andra medlemsstaten för alla belopp den har betalat ut till offren eller de personer som befullmäktigats att handla på offrens vägnar.

4. När en medlemsstats tjänstemän verkar i en annan medlemsstat i enlighet med artikel 18, ska den sistnämnda medlemsstaten i enlighet med sin nationella lagstiftning ansvara för de eventuella skador som de förorsakar under sina insatser.

5. När den skada som avses i punkt 4 följer av grov oaktsamhet eller avsiktlig försummelse, får värdmedlemsstaten begära att hemmedlemsstaten ska ersätta de belopp som värdmedlemsstaten har betalat ut för att gottgöra offren eller de personer som på offrens vägnar har rätt till ersättning.

6. Utan att det påverkar utövandet av eventuella rättigheter gentemot tredje part och med undantag för vad som sägs i punkt 3 ska alla medlemsstater under de omständigheter som avses i punkt 1 avstå från att kräva ersättning för de skador den lidit av en annan medlemsstat.

Artikel 22

Straffrättsligt ansvar

Tjänstemän som enligt detta beslut verkar på en annan medlemsstats territorium ska i fråga om brott som de begår eller brott som de utsätts för jämställas med den andra medlemsstatens tjänstemän, om inte annat följer av något annat avtal som är bindande för de berörda medlemsstaterna.

Artikel 23

Tjänsteförhållanden

Tjänstemän som enligt detta beslut verkar på en annan medlemsstats territorium ska i tjänsterättsligt hänseende, särskilt vad gäller de disciplinära bestämmelserna, omfattas av den tillämpliga lagstiftningen i sin egen medlemsstat.

KAPITEL 6

ALLMÄNNA BESTÄMMELSER OM DATASKYDD

Artikel 24

Definitioner och tillämpningsområde

1. I detta beslut gäller följande definitioner:

a) *behandling av personuppgifter*: all behandling av personuppgifter eller en räcka behandlingar med eller utan hjälp av automatiska förfaranden, såsom insamling, registrering, organisering, lagring, bearbetning eller ändring, urval, förfrågan, konsultering, användning, överlåtelse genom överföring, spridning och alla andra former av tillhandahållande, kombination eller sammankoppling samt spärrande, avförande eller utplånande av uppgifter. Som behandling av personuppgifter enligt detta beslut anses även underrättelse om huruvida en överensstämmelse konstaterats eller inte.

b) *automatisk sökning*: direkt tillträde till ett annat organs automatiska databas på ett sätt där en förfrågan besvaras fullständigt automatiskt.

c) *förseende med en beteckning*: märkning av registrerade personuppgifter som inte syftar till att begränsa den framtida behandlingen av dem.

d) *spärrande*: märkning av registrerade personuppgifter i syfte att begränsa den framtida behandlingen av dem.

2. Följande bestämmelser ska gälla för uppgifter som översänds eller har översänts enligt detta beslut, om inte annat föreskrivs i de föregående kapitlen.

Artikel 25

Dataskyddsnivå

1. Varje medlemsstat ska i sin nationella lagstiftning, i fråga om behandlingen av personuppgifter som översänds eller har översänts enligt detta beslut, garantera ett skydd för personuppgifter som motsvarar åtminstone den nivå som fastställs i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter och i tilläggsprotokollet av den 8 november 2001, och ska därvid beakta rekommendation nr R (87) 15 av den 17 september 1987 från Europarådets ministerkommitté till medlemsstaterna om polisens användning av personuppgifter, även när uppgifterna inte behandlas automatiskt.

2. Översändande av personuppgifter i enlighet med detta beslut får inledas först när bestämmelserna i detta kapitel har genomförts i lagstiftningen i de medlemsstater som deltar i informationsutbytet. Rådet ska enhälligt besluta om huruvida denna förutsättning är uppfylld.

3. Punkt 2 ska inte tillämpas på de medlemsstater där översändandet av personuppgifter enligt detta beslut redan har inletts i enlighet med fördraget av den 27 maj 2005 mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (Prümfördraget).

Artikel 26

Syfte

1. Den mottagande medlemsstaten får behandla personuppgifter endast för de syften för vilka uppgifterna har översänts i enlighet med detta beslut. Behandling för andra syften ska vara tillåten endast med förhandstillstånd från den medlemsstat som administrerar uppgifterna och i enlighet med den mottagande medlemsstatens nationella lagstiftning. Ett sådant tillstånd får beviljas om den nationella lagstiftningen i den medlemsstat som administrerar uppgifterna tillåter denna behandling för sådana andra syften.

2. Den sökande eller jämförande medlemsstaten får behandla uppgifter som översänts i enlighet med artiklarna 3, 4 och 9 endast för

a) fastställande av om jämförda DNA-profiler eller fingeravtrycksuppgifter överensstämmer,

b) utarbetande och inlämnande av en begäran om handräckning eller rättslig hjälp i enlighet med den nationella lagstiftningen när dessa uppgifter överensstämmer,

c) registrering i enlighet med artikel 30.

Den medlemsstat som administrerar uppgifterna får behandla uppgifter som översänts till den i enlighet med artiklarna 3, 4 och 9 endast om det är nödvändigt för att göra en jämförelse, svara på en automatisk sökning eller göra en registrering enligt artikel 30. Efter det att jämförelsen av uppgifter avslutats eller den automatiska sökningen besvarats ska de uppgifter som översänts omedelbart utplånas, om det inte är nödvändigt med en ytterligare behandling av dem för de syften som anges i leden b och c i första stycket.

3. Den medlemsstat som administrerar uppgifterna får använda uppgifter som översänts i enlighet med artikel 12 endast om det är nödvändigt för besvarande av en automatisk sökning eller för registrering i enlighet med artikel 30. Efter det att den automatiska sökningen besvarats ska de uppgifter som översänts omedelbart utplånas, om det inte är nödvändigt med en ytterligare behandling av dem för registrering i enlighet med artikel 30. Den sökande medlemsstaten får använda de uppgifter som erhållits under sökningen endast för det förfarande på grundval av vilket sökningen skett.

Artikel 27

Behöriga myndigheter

Översända personuppgifter får endast behandlas av de myndigheter, organ och domstolar som ansvarar för en uppgift i enlighet med syftena i artikel 26. Särskilt får uppgifter översändas till andra myndigheter endast med den översändande medlemsstatens förhandstillstånd och i enlighet med den mottagande medlemsstatens nationella lagstiftning.

Artikel 28

Uppgifternas korrekthet, aktualitet och lagringstid

1. Medlemsstaterna ska säkerställa att personuppgifterna är korrekta och aktuella. Om det *ex officio* eller genom ett meddelande från den berörda personen visar sig att felaktiga uppgifter eller uppgifter som inte borde ha översänts har översänts, ska den eller de mottagande medlemsstaterna omedelbart underrättas om detta. Den eller de berörda medlemsstaterna ska vara skyldiga att rätta eller utplåna uppgifterna. Även i övriga fall ska översända personuppgifter rättas om det framgår att de är felaktiga. Om det mottagande organet har skäl att anta att de översända uppgifterna är felaktiga eller bör utplånas ska den utan dröjsmål underrätta det översändande organet om detta.

2. Uppgifter vars korrekthet den berörda personen bestrider och vars korrekthet eller felaktighet inte kan fastställas ska märkas, i enlighet med medlemsstaternas nationella lagstiftning, på begäran av den person som uppgifterna berör. Om en sådan märkning har använts får denna avlägsnas, i enlighet med medlemsstaternas nationella lagstiftning, endast med den berörda personens medgivande eller genom beslut av en behörig domstol eller en oberoende myndighet som ansvarar för övervakningen av dataskyddet.

3. Översända personuppgifter ska utplånas om de inte borde ha översänts eller mottagits. Uppgifter som har översänts och mottagits korrekt ska utplånas

a) om de inte eller inte längre är nödvändiga för det syfte för vilket de översänts; om personuppgifterna har översänts utan begäran ska det mottagande organet omedelbart kontrollera om de är nödvändiga med tanke på de syften för vilka de översändes,

b) efter det att den tidsfrist som fastställs för lagring av uppgifterna enligt den översändande medlemsstatens nationella lagstiftning har löpt ut, när det översändande organet har informerat det mottagande organet om denna maximala lagringstid i samband med att uppgifterna översändes.

I stället för att utplånas ska uppgifterna spärras i enlighet med den nationella lagstiftningen om det finns skäl att anta att en utplåning skulle skada den berörda personens intressen. Spärrade uppgifter får endast översändas eller användas i det syfte som lett till att utplåningen förhindrades.

Artikel 29

Tekniska och organisatoriska åtgärder för säkerställande av dataskydd och datasäkerhet

1. De översändande och mottagande organen ska vidta åtgärder så att personuppgifter skyddas effektivt mot oavsiktlig eller otillåten utplåning, oavsiktlig förlust, obehörig tillgång, obehörig eller oavsiktlig ändring och obehörigt offentliggörande.

2. Detaljerna för det automatiska sökningsförfarandet ska fastställas i de genomförandeåtgärder som avses i artikel 33, som garanterar att

a) åtgärder som motsvarar den senaste tekniken vidtas för att säkerställa dataskydd och datasäkerhet, särskilt uppgifternas konfidentialitet och integritet,

b) krypterings- och autentiseringsmetoder som erkänns av de behöriga myndigheterna används när allmänt tillgängliga nät utnyttjas, och

c) det i enlighet med artikel 30.2, 30.4 och 30.5 kan kontrolleras att sökningarna är tillåtna.

Artikel 30

Registrering och dokumentation, särskilda bestämmelser om automatiskt och icke-automatiskt översändande

1. Varje medlemsstat ska garantera att varje icke-automatiskt översändande och varje icke-automatiskt mottagande av personuppgifter i det organ som administrerar databasen och i det sökande organet registreras för att kontrollera att sändningen är tillåten. Registreringen ska omfatta följande uppgifter:

a) Skälet till översändandet.

b) Översända uppgifter.

c) Datum för översändandet.

d) Namn eller sifferbeteckning på det sökande organet och det organ som administrerar databasen.

2. För automatisk sökning av uppgifter i enlighet med artiklarna 3, 9 och 12 och för automatisk jämförelse i enlighet med artikel 4 ska följande gälla:

a) En automatisk sökning eller jämförelse får endast genomföras av de tjänstemän vid nationella kontaktställen som särskilt bemyndigats att göra detta. En förteckning över de tjänstemän som bemyndigats att genomföra automatiska sökningar eller jämförelser ska på begäran ställas till förfogande för de övervakningsmyndigheter som avses i punkt 5 och de övriga medlemsstaterna.

b) Varje medlemsstat ska garantera att varje översändande och mottagande av personuppgifter i det organ som administrerar databasen och i det sökande organet registreras tillsammans med uppgift om huruvida sökningen lett till en träff eller inte. Denna registrering ska omfatta följande uppgifter:

i) Översända uppgifter.

ii) Datum och exakt tidpunkt för översändandet.

iii) Namn eller sifferbeteckning på det sökande organet och det organ som administrerar databasen.

Det sökande organet ska dessutom registrera sökningens eller översändandets syfte samt en identitetsuppgift för den tjänsteman som initierade sökningen eller översändandet.

3. Det registrerande organet ska på begäran utan dröjsmål delge den berörda medlemsstatens behöriga dataskyddsmyndigheter de registrerade uppgifterna, dock senast fyra veckor efter det att begäran inkom. De registrerade uppgifterna får endast användas för följande ändamål:

a) Övervakning av dataskydd.

b) Garanterande av datasäkerheten.

4. De registrerade uppgifterna ska med hjälp av lämpliga åtgärder skyddas mot obehörig användning och andra former av missbruk och lagras i två år. När lagringstiden har löpt ut ska de registrerade uppgifterna utan dröjsmål utplånas.

5. Den rättsliga övervakningen av översändande och mottagande av personuppgifter ska ankomma på de oberoende dataskyddsmyndigheterna eller, i förekommande fall, de rättsliga myndigheterna i varje medlemsstat. I enlighet med den nationella lagstiftningen kan var och en hos dessa myndigheter ansöka om en granskning av lagligheten beträffande behandlingen av sina personuppgifter. Dessa myndigheter och de organ som ansvarar för registreringen ska även oberoende av ovan nämnda ansökningar göra stickprov för att kontrollera översändningarnas laglighet med hjälp av berörda dokument.

De oberoende dataskyddsmyndigheterna ska förvara resultaten av dessa kontroller för granskning i 18 månader. Efter denna tidsfrist ska de utplånas omedelbart. Varje dataskyddsmyndighet kan anmodas av den oberoende dataskyddsmyndigheten i en annan medlemsstat att utöva sina befogenheter i enlighet med den nationella lagstiftningen. Medlemsstaternas oberoende dataskyddsmyndigheter ska utföra de inspektioner som är nödvändiga för det ömsesidiga samarbetet, särskilt genom utbyte av relevant information.

Artikel 31

Berörda personers rätt till information och skadestånd

1. På begäran av den berörda personen i enlighet med nationell lagstiftning ska denna person som bevisar sin identitet, utan oskäliga avgifter, i en allmänt förståelig form och utan oacceptabla dröjsmål, i enlighet med nationell lagstiftning informeras om de uppgifter om denna person som har varit föremål för behandling, liksom om uppgifternas ursprung, mottagare eller kategori av mottagare, det avsedda ändamålet med behandlingen och, när så krävs i nationell lagstiftning, dess rättsliga grund. Dessutom ska den person som uppgifterna berör ha rätt att kräva att felaktiga uppgifter korrigeras och att uppgifter som behandlats på otillbörligt sätt utplånas. Medlemsstaterna ska dessutom säkerställa att den person som uppgifterna berör, då personens rättigheter avseende dataskydd kränkts, kan överklaga hos en oavhängig domstol enligt artikel 6.1 i den europeiska konventionen om de mänskliga rättigheterna eller hos en oberoende tillsynsmyndighet enligt artikel 28 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([1]), och att personen ges möjlighet att kräva skadestånd eller annan ersättning. De närmare bestämmelserna för förfarandet för att hävda dessa rättigheter och skälen till begränsning av tillgången ska följa den tillämpliga nationella lagstiftningen i den medlemsstat där personen i fråga hävdar sina rättigheter.

2. När ett organ i en medlemsstat har översänt personuppgifter i enlighet med detta beslut, kan den mottagande myndigheten i en annan medlemsstat inte hänvisa till att de översända uppgifterna var felaktiga för att undgå sitt ansvar gentemot den skadelidande i enlighet med den nationella lagstiftningen. Om det mottagande organet döms att betala skadestånd på grund av dess användning av översända felaktiga uppgifter ska det översändande organet ersätta det mottagande organets skadeståndsbetalning till fullt belopp.

Artikel 32

Information på begäran av medlemsstaterna

Den mottagande medlemsstaten ska på begäran ge den översändande medlemsstaten information om behandlingen av de översända uppgifterna och de resultat som erhållits.

KAPITEL 7

GENOMFÖRANDE OCH SLUTBESTÄMMELSER

Artikel 33

Genomförandeåtgärder

Rådet ska, med kvalificerad majoritet och efter att ha hört Europaparlamentet, besluta om de åtgärder som är nödvändiga för att genomföra detta beslut på unionsnivå.

([1]) EGT L 281, 23.11.1995, s. 31. Direktivet ändrat genom förordning (EG) nr 1882/2003 (EUT L 284, 31.10.2003, s. 1.)

Artikel 34

Kostnader

Varje medlemsstat ska ansvara för de driftskostnader som dess egna myndigheter ådrar sig i samband med tillämpningen av detta beslut. I särskilda fall får de berörda medlemsstaterna komma överens om avvikande arrangemang.

Artikel 35

Förhållandet till andra instrument

1. För de berörda medlemsstaterna ska de tillämpliga bestämmelserna i detta beslut tillämpas i stället för motsvarande bestämmelser i Prümfördraget. Varje annan bestämmelse i Prümfördraget ska fortfarande vara tillämplig mellan de fördragsslutande parterna i Prümfördraget.

2. Medlemsstaterna får, utan att det påverkar deras åtaganden enligt andra rättakter som antagits enligt avdelning VI i fördraget,

a) fortsätta att tillämpa bilaterala eller multilaterala avtal eller överenskommelser om gränsöverskridande samarbete som är i kraft den dag då detta beslut antas, förutsatt att dessa avtal eller överenskommelser inte är oförenliga med målen för detta beslut,

b) ingå eller låta träda i kraft bilaterala eller multilaterala avtal eller överenskommelser om gränsöverskridande samarbete efter det att detta beslut har trätt i kraft, förutsatt att dessa avtal eller överenskommelser gör det möjligt att utvidga eller bredda målen för detta beslut.

3. De avtal och överenskommelser som avses i punkterna 1 och 2 får inte påverka förbindelserna med de medlemsstater som inte är parter i dem.

4. Medlemsstaterna ska inom fyra veckor efter det att detta beslut fått verkan underrätta rådet och kommissionen om de befintliga avtal eller överenskommelser enligt punkt 2 a som de vill fortsätta att tillämpa.

5. Medlemsstaterna ska också underrätta rådet och kommissionen om alla nya avtal eller överenskommelser enligt punkt 2 b inom tre månader efter undertecknandet eller, om det gäller instrument som undertecknades innan detta beslut antogs, inom tre månader efter deras ikraftträdande.

6. Ingenting i detta beslut ska påverka bilaterala eller multilaterala avtal eller överenskommelser mellan medlemsstaterna och tredjestater.

7. Detta beslut ska inte påverka befintliga avtal om rättslig hjälp eller ömsesidigt erkännande av domstolsavgöranden.

Artikel 36

Genomförande och förklaringar

1. Medlemsstaterna ska vidta nödvändiga åtgärder för att följa bestämmelserna i detta beslut inom ett år efter det att beslutet har fått verkan, med undantag av bestämmelserna i kapitel 2 avseende vilka nödvändiga åtgärder ska vidtas inom tre år efter det att detta beslut och rådets beslut om tillämpningen av detta beslut har fått verkan.

2. Medlemsstaterna ska underrätta rådets generalsekretariat och kommissionen om att de har uppfyllt de skyldigheter som de åläggs enligt detta beslut och lämna in de förklaringar som avses i beslutet. I samband med detta får varje medlemsstat meddela att den omedelbart kommer att tillämpa detta beslut i förbindelserna med de medlemsstater som har lämnat samma meddelande.

3. Förklaringar som har lämnats i enlighet med punkt 2 får när som helst ändras genom en förklaring som lämnas till rådets generalsekretariat. Rådets generalsekretariat ska vidarebefordra alla mottagna förklaringar till medlemsstaterna och kommissionen.

4. På grundval av detta och annan information som medlemsstaterna gjort tillgänglig på begäran ska kommissionen inge en rapport till rådet senast den 28 juli 2012 om genomförandet av detta beslut åtföljd av förslag som den anser lämpliga för vidare utveckling.

Artikel 37

Tillämpning

Detta beslut får verkan tjugo dagar efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Luxemburg den 23 juni 2008.

På rådets vägnar

I. JARC

Ordförande

RÅDETS BESLUT 2008/616/RIF

av den 23 juni 2008

om genomförande av beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet

EUROPEISKA UNIONENS RÅD HAR BESLUTAT FÖLJANDE

med beaktande av artikel 33 i rådets beslut 2008/615/RIF ([1]),

med beaktande av initiativet från Förbundsrepubliken Tyskland,

med beaktande av Europaparlamentets yttrande ([2]), och

av följande skäl:

(1) Den 23 juni 2008 antog rådet beslut 2008/615/RIF om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet.

(2) Genom beslut 2008/615/RIF införlivades de väsentliga delarna av fördraget av den 27 maj 2005 mellan Konungariket Belgien, Förbundsrepubliken Tyskland, Konungariket Spanien, Republiken Frankrike, Storhertigdömet Luxemburg, Konungariket Nederländerna och Republiken Österrike om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration (nedan kallat *Prümfördraget*) med Europeiska unionens rättsliga ram.

(3) Enligt artikel 33 i beslut 2008/615/RIF ska rådet besluta om de åtgärder som är nödvändiga för att genomföra beslut 2008/615/RIF på unionsnivå i enlighet med förfarandet i artikel 34.2 c andra meningen i fördraget om Europeiska unionen. Dessa åtgärder ska bygga på genomförandeavtalet av den 5 december 2006 beträffande de administrativa och tekniska aspekterna av genomförandet och tillämpningen av Prümfördraget.

(4) I beslutet fastställs de gemensamma normativa bestämmelser som är absolut nödvändiga för det administrativa och tekniska genomförandet av de samarbetsformer som anges i beslut 2008/615/RIF. Bilagan till det här beslutet innehåller genomförandebestämmelser av teknisk karaktär. En separat handbok, som endast innehåller faktauppgifter som ska lämnas av medlemsstaterna, kommer dessutom att utarbetas och hållas uppdaterad av rådets generalsekretariat.

(5) Med beaktande av de tekniska resurserna kommer rutinsökningar av nya DNA-profiler i princip att genomföras med hjälp av enstaka sökningar och lämpliga lösningar för detta kommer att sökas på teknisk nivå.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte

Syftet med detta beslut är att fastställa de nödvändiga administrativa och tekniska bestämmelserna för genomförandet av beslut 2008/615/RIF, särskilt för det automatiska utbytet av DNA-uppgifter, fingeravtrycksuppgifter och uppgifter ur fordonsregister enligt kapitel 2 i det beslutet samt för andra samarbetsformer enligt kapitel 5 i det beslutet.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner

a) *sökning* och *jämförelse* enligt artiklarna 3, 4 och 9 i beslut 2008/615/RIF: de förfaranden genom vilka det fastställs om det finns någon överensstämmelse mellan DNA-uppgifter eller fingeravtrycksuppgifter som har lämnats av en medlemsstat och DNA-uppgifter eller fingeravtrycksuppgifter som finns lagrade i en, flera eller samtliga medlemsstaters databaser.

b) *automatisk sökning* enligt artikel 12 i beslut 2008/615/RIF: förfarande för tillgång online för att söka i en, flera eller samtliga medlemsstaters databaser.

c) *DNA-profil*: en bokstav eller en nummerkod som representerar en rad identifikationsuppgifter i den icke-kodifierande delen av ett analyserat mänskligt DNA-prov, dvs. den särskilda molekylära strukturen vid de olika DNA-lokusen.

d) *icke-kodifierande del av DNA*: kromosomområden som inte innehåller någon genetisk information, dvs. inga hänvisningar till en organisms funktionella egenskaper.

([1]) Se sidan 1 i detta nummer av EUT.

([2]) Yttrandet avgivet den 21 april 2008 (ännu ej offentliggjort i EUT).

e) *DNA-referensuppgifter*: en DNA-profil och en sifferbeteckning.

f) *DNA-personprofil*: DNA-profilen för en identifierad person.

g) *oidentifierad DNA-profil*: den DNA-profil som erhålls från spår som samlats in under brottsutredningen och tillhör en person som ännu inte identifierats.

h) *notering*: en medlemsstats markering i en DNA-profil i den nationella databasen om att man redan konstaterat en överensstämmelse för en sådan DNA-profil vid en annan medlemsstats sökning eller jämförelse.

i) *fingeravtrycksuppgifter*: fingeravtrycksbilder, dolda fingeravtrycksbilder, handavtryck, dolda handavtryck samt modeller för sådana bilder (kodade detaljer), när de lagras och hanteras i en automatisk databas.

j) *uppgifter ur fordonsregister*: uppsättningen uppgifter enligt kapitel 3 i bilagan till detta beslut.

k) *enskilda fall* enligt artiklarna 3.1 andra meningen, 9.1 andra meningen och 12.1 i beslut 2008/615/RIF: en enda utrednings- eller lagföringsfil. Om en sådan fil innehåller mer än en DNA-profil, fingeravtrycksuppgift eller uppgift ur fordonsregister ska dessa översändas tillsammans som en begäran.

KAPITEL 2

GEMENSAMMA BESTÄMMELSER OM UTBYTE AV UPPGIFTER

Artikel 3

Tekniska specifikationer

Medlemsstaterna ska följa de gemensamma tekniska specifikationerna i samband med varje begäran och svar som gäller sökningar och jämförelser av DNA-profiler, fingeravtrycksuppgifter och uppgifter ur fordonsregister. Dessa tekniska specifikationer fastställs i bilagan till detta beslut.

Artikel 4

Kommunikationsnät

Det elektroniska utbytet av DNA-uppgifter, fingeravtrycksuppgifter och uppgifter ur fordonsregister mellan medlemsstaterna ska ske med hjälp av kommunikationsnätet för de transeuropeiska tjänsterna för telematik mellan förvaltningarnas (Testa II) och vidareutveckling av dessa.

Artikel 5

Tillgång till automatiskt utbyte av uppgifter

Medlemsstaterna ska vidta alla nödvändiga åtgärder för att säkerställa att automatisk sökning eller jämförelse av DNA-uppgifter, fingeravtrycksuppgifter och uppgifter ur fordonsregister är möjlig dygnet runt sju dagar i veckan. Vid tekniskt fel ska medlemsstaternas nationella kontaktpunkter omedelbart underrätta varandra och enas om system för tillfälligt alternativt informationsutbyte i enlighet med de tillämpliga rättsliga bestämmelserna. Automatiskt utbyte av uppgifter ska återupprättas så snabbt som möjligt.

Artikel 6

Sifferbeteckningar för DNA-uppgifter och fingeravtrycksuppgifter

De sifferbeteckningar som avses i artiklarna 2 och 8 i beslut 2008/615/RIF ska bestå av en kombination av följande:

a) En kod som gör det möjligt för medlemsstaterna att om en överensstämmelse konstaterats hämta personuppgifter och ytterligare information från sina databaser för vidarebefordran till en, flera eller samtliga medlemsstater i enlighet med artikel 5 eller artikel 10 i beslut 2008/615/RIF.

b) En kod för att ange DNA-profilens eller fingeravtrycksuppgifternas nationella ursprung.

c) För DNA-uppgifter, en kod för att ange typen av DNA-profil.

KAPITEL 3

DNA-UPPGIFTER

Artikel 7

Principer för utbyte av DNA-uppgifter

1. Medlemsstaterna ska använda befintliga standarder för utbyte av DNA-uppgifter, till exempel den europeiska standarduppsättningen (ESS) eller Interpols standarduppsättning med lokus (Issol).

2. Översändandet ska vid automatisk sökning och jämförelse av DNA-uppgifter ske inom en decentraliserad struktur.

3. Lämpliga åtgärder ska vidtas för att säkerställa konfidentialiteten och integriteten för de uppgifter som översänds till andra medlemsstater, inklusive krypteringen av dessa.

4. Medlemsstaterna ska vidta nödvändiga åtgärder för att garantera integriteten för de DNA-profiler som görs tillgängliga eller skickas för jämförelse till de andra medlemsstaterna och säkerställa att dessa åtgärder överensstämmer med internationella standarder, exempelvis ISO 17025.

5. Medlemsstaterna ska använda medlemsstatskoder enligt ISO-standarden 3166-1 tvåbokstavskod.

Artikel 8

Regler för begäran och svar i samband med DNA-uppgifter

1. En begäran om en automatisk sökning eller jämförelse enligt artikel 3 eller 4 i beslut 2008/615/RIF ska endast innehålla följande information:

a) Den begärande medlemsstatens medlemsstatskod.

b) Dag, tid och referensnummer för begäran.

c) DNA-profiler och deras sifferbeteckning.

d) Typer av DNA-profiler som har översänts (oidentifierade DNA-profiler eller DNA-personprofiler).

e) Information som krävs för att kontrollera databassystemen och kvalitetskontroll för de automatiska sökprocesserna.

2. Svaret (rapporten om de automatiska sökprocesserna överensstämmelse) på en begäran enligt punkt 1 ska endast innehålla följande information:

a) Uppgift om det finns ett eller flera fall av överensstämmelse (träffar) eller inte (ingen träff).

b) Dag, tid och referensnummer för begäran.

c) Dag, tid och referensnummer för svaret.

d) De begärande och de anmodade medlemsstaternas medlemsstatskoder.

e) De begärande och de anmodade medlemsstaternas sifferbeteckningar.

f) Den typ av DNA-profiler som översänds (oidentifierade DNA-profiler eller DNA-personprofiler).

g) De begärda och överensstämmande DNA-profilerna.

h) Information som krävs för att kontrollera databassystemen och kvalitetskontroll för de automatiska sökprocesserna.

3. En överensstämmelse ska meddelas automatiskt endast om den automatiska sökningen eller jämförelsen har resulterat i en överensstämmelse mellan ett minimiantal lokus. Detta minimiantal fastställs i kapitel 1 i bilagan till detta beslut.

4. Medlemsstaterna ska se till att begäran överensstämmer med de förklaringar som lämnats enligt artikel 2.3 i beslut 2008/615/RIF. Förklaringarna ska återges i den handbok som avses i artikel 18.2 i detta beslut.

Artikel 9

Översändandeförfarande för automatisk sökning av oidentifierade DNA-profiler i enlighet med artikel 3 i beslut 2008/615/RIF

1. Om man vid en sökning med en oidentifierad DNA-profil inte har konstaterat någon överensstämmelse i den nationella databasen, eller man har konstaterat överensstämmelse med en oidentifierad DNA-profil, får den oidentifierade DNA-profilen översändas till alla övriga medlemsstaters databaser, och om man vid en sökning med denna oidentifierade DNA-profil konstaterar överensstämmelser med DNA-personprofiler och/eller oidentifierade DNA-profiler i andra medlemsstaters databaser, ska dessa överensstämmelser automatiskt meddelas och DNA-referensuppgifterna översändas till den begärande medlemsstaten. Om man inte kan konstatera någon överensstämmelse i andra medlemsstaters databaser, ska detta automatiskt meddelas den begärande medlemsstaten.

2. Om man vid en sökning med en oidentifierad DNA-profil konstaterar en överensstämmelse i andra medlemsstaters databaser får varje berörd medlemsstat föra in en notering om detta i sin nationella databas.

Artikel 10

Översändandeförfarande för automatisk sökning av DNA-personprofiler i enlighet med artikel 3 i beslut 2008/615/RIF

Om man vid en sökning med en DNA-personprofil inte har konstaterat någon överensstämmelse i den nationella databasen med en DNA-personprofil eller konstaterat en överensstämmelse med en oidentifierad DNA-profil, får denna DNA-personprofil översändas till alla övriga medlemsstaters databaser, och om man vid en sökning med denna DNA-personprofil konstaterar överensstämmelser med DNA-personprofiler och/eller oidentifierade DNA-profiler i andra medlemsstaters databaser ska dessa överensstämmelser automatiskt meddelas och DNA-referensuppgifterna översändas till den begärande medlemsstaten. Om man inte kan konstatera någon överensstämmelse i andra medlemsstaters databaser, ska detta automatiskt meddelas den begärande medlemsstaten.

Artikel 11

Översändandeförfarande för automatisk jämförelse av oidentifierade DNA-profiler i enlighet med artikel 4 i beslut 2008/615/RIF

1. Om man vid en jämförelse med oidentifierade DNA-profiler konstaterar överensstämmelser med DNA-personprofiler och/eller oidentifierade DNA-profiler i andra medlemsstaters databaser ska dessa överensstämmelser automatiskt meddelas och DNA-referensuppgifterna översändas till den begärande medlemsstaten.

2. Om man vid en jämförelse med oidentifierade DNA-profiler konstaterar överensstämmelser med oidentifierade DNA-profiler eller DNA-personprofiler i andra medlemsstaters databaser får varje berörd medlemsstat införa en notering om detta i sin nationella databas.

KAPITEL 4

FINGERAVTRYCKSUPPGIFTER

Artikel 12

Principer för utbyte av fingeravtrycksuppgifter

1. Digitalisering av fingeravtrycksuppgifter och översändandet av dessa till de övriga medlemsstaterna ska genomföras i enlighet med ett enhetligt dataformat som specificeras i kapitel 2 i bilagan till detta beslut.

2. Varje medlemsstat ska se till att de fingeravtrycksuppgifter som den översänder har tillräckligt god kvalitet för att kunna jämföras med hjälp av de automatiska fingeravtrycksidentifieringssystemen (Afis).

3. Översändandeförfarandet för utbyte av fingeravtrycksuppgifter ska ske inom en decentraliserad struktur.

4. Lämpliga åtgärder ska vidtas för att säkerställa konfidentialiteten och integriteten för de fingeravtrycksuppgifter som översänds till andra medlemsstater, inklusive krypteringen av dessa.

5. Medlemsstaterna ska använda medlemsstatskoder i enlighet med ISO-standard 3166-1 tvåbokstavskod.

Artikel 13

Sökningskapacitet för fingeravtrycksuppgifter

1. Varje medlemsstat ska se till att dess begäran om sökning inte överskrider den sökningskapacitet som specificerats av den anmodade medlemsstaten. Medlemsstaterna ska lämna förklaringar som anges i artikel 18.2 till rådets generalsekretariat i vilka de fastställer sin maximala sökningskapacitet per dag för fingeravtrycksuppgifter om identifierade personer eller för fingeravtrycksuppgifter om ännu inte identifierade personer.

2. Det maximala antalet personer som godtas för kontroll per översändande fastställs i kapitel 2 i bilagan till detta beslut.

Artikel 14

Regler för begäran och svar i samband med fingeravtrycksuppgifter

1. Den anmodade medlemsstaten ska utan dröjsmål kontrollera kvaliteten på de översända fingeravtrycksuppgifterna genom ett helt automatiskt förfarande. Om uppgifterna inte lämpar sig för en automatisk jämförelse, ska den anmodade medlemsstaten omedelbart underrätta den begärande medlemsstaten.

2. Den anmodade medlemsstaten ska utföra sökningar i den ordning som den får begäran. Begäran ska behandlas inom 24 timmar genom ett helt automatiskt förfarande. Den begärande medlemsstaten får, om dess nationella lagstiftning så föreskriver, begära att behandlingen av dess begäran påskyndas och den anmodade medlemsstaten ska utföra dessa sökningar utan dröjsmål. Om tidsfristerna inte kan hållas på grund av *force majeure*, ska jämförelsen göras utan dröjsmål så snart som hindren har avlägsnats.

KAPITEL 5

UPPGIFTER UR FORDONSREGISTER

Artikel 15

Principer för automatisk sökning av uppgifter ur fordonsregister

1. För automatisk sökning av uppgifter ur fordonsregister ska medlemsstaterna använda en enligt artikel 12 i beslut 2008/615/RIF särskilt utarbetad version av programvaran för det europeiska informationssystemet avseende fordon och körkort (Eucaris) och ändrade versioner av denna programvara.

2. Automatisk sökning av uppgifter ur fordonsregister ska ske inom en decentraliserad struktur.

3. De uppgifter som utbyts via Eucaris-systemet ska översändas i krypterad form.

4. De delar av uppgifterna ur fordonsregistret som ska utbytas specificeras i kapitel 3 i bilagan till detta beslut.

5. Vid tillämpningen av artikel 12 i beslut 2008/615/RIF får medlemsstaterna prioritera sökningar i syfte att bekämpa allvarlig brottslighet.

Artikel 16

Kostnader

Varje medlemsstat ska ansvara för kostnaderna för administrationen, användningen och underhållet av den version av programvaran för Eucaris som anges i artikel 15.1.

KAPITEL 6

POLISSAMARBETE

Artikel 17

Gemensam patrullering och andra gemensamma insatser

1. Enligt kapitel 5 i beslut 2008/615/RIF, särskilt de förklaringar som lämnats enligt artiklarna 17.4, 19.2 och 19.4 i det beslutet, ska varje medlemsstat utse en eller flera kontaktpunkter

så att andra medlemsstater kan vända sig till de behöriga myndigheterna och varje medlemsstat får specificera sina förfaranden för att inleda gemensam patrullering och andra gemensamma insatser, sina förfaranden för initiativ från andra medlemsstater när det gäller dessa insatser samt andra praktiska aspekter och operativa regler i samband med dessa insatser.

2. Rådets generalsekretariat ska sammanställa och uppdatera en förteckning över kontaktpunkterna och underrätta de behöriga myndigheterna om eventuella ändringar i förteckningen.

3. De behöriga myndigheterna i varje medlemsstat får ta initiativ till att inleda en gemensam insats. Innan en specifik insats inleds, ska de behöriga myndigheter som avses i punkt 2 skriftligen eller muntligen vidta arrangemang som till exempel kan avse

a) de behöriga myndigheterna i de medlemsstater som ansvarar för insatsen,

b) insatsens specifika syfte,

c) den värdmedlemsstat där insatsen äger rum,

d) det geografiska området i den värdmedlemsstat där insatsen äger rum,

e) den period som insatsen avser,

f) det särskilda bistånd som den utsändande medlemsstaten/de utsändande medlemsstaterna ska tillhandahålla värdmedlemsstaten, bl.a. tjänstemän eller andra statsanställda, materiel och finansiella inslag,

g) de tjänstemän som deltar i insatsen,

h) den tjänsteman som leder insatsen,

i) de befogenheter som den utsändande medlemsstatens/de utsändande medlemsstaternas tjänstemän eller andra statsanställda får utöva i värdmedlemsstaten under insatsen,

j) vissa tjänstevapen, viss ammunition och utrustning som de utsända tjänstemännen får använda under insatsen enligt beslut 2008/615/RIF,

k) regler för logistiken kring transport, inkvartering och säkerhet,

l) ansvaret för kostnaderna för den gemensamma insatsen vid avvikelse från vad som föreskrivs i artikel 34 första meningen i beslut 2008/615/RIF,

m) eventuella övriga inslag som krävs.

4. De förklaringar, förfaranden och utseenderegler som föreskrivs i denna artikel ska återges i den handbok som avses i artikel 18.2.

KAPITEL 7

SLUTBESTÄMMELSER

Artikel 18

Bilaga och handbok

1. Ytterligare uppgifter om det tekniska och administrativa genomförandet av beslut 2008/615/RIF återfinns i bilagan till det här beslutet.

2. En handbok ska utarbetas och hållas uppdaterad av rådets generalsekretariat samt endast innehålla faktauppgifter som lämnas av medlemsstaterna genom förklaringar i enlighet med beslut 2008/615/RIF eller det här beslutet eller genom anmälningar till rådets generalsekretariat. Handboken ska ha formen av ett rådsdokument.

Artikel 19

Oberoende dataskyddsmyndigheter

Medlemsstaterna ska, i enlighet med artikel 18.2 i detta beslut, informera rådets generalsekretariat om de oberoende dataskyddsmyndigheter eller de rättsliga myndigheter som avses i artikel 30.5 i beslut 2008/615/RIF.

Artikel 20

Förberedelse av beslut enligt artikel 25.2 i beslut 2008/615/RIF

1. Rådet ska fatta ett beslut enligt artikel 25.2 i beslut 2008/615/RIF på grundval av en utvärderingsrapport som ska grundas på ett frågeformulär.

2. Med beaktande av det automatiska utbytet av uppgifter i enlighet med kapitel 2 i beslut 2008/615/RIF ska utvärderingsrapporten även grundas på ett utvärderingsbesök och en testkörning som ska genomföras när den berörda medlemsstaten har informerat generalsekretariatet enligt artikel 36.2 första meningen i beslut 2008/615/RIF.

3. Närmare uppgifter om förfarandet anges i kapitel 4 i bilagan till detta beslut.

Artikel 21

Utvärdering av utbytet av uppgifter

1. En utvärdering av den administrativa, tekniska och finansiella tillämpningen av utbytet av uppgifter enligt kapitel 2 i beslut 2008/615/RIF, särskilt användningen av mekanismen i artikel 15.5, ska genomföras regelbundet. Utvärderingen ska omfatta de medlemsstater som redan tillämpar beslut 2008/615/RIF vid tiden för utvärderingen och beakta de uppgiftskategorier för

vilka utbytet av uppgifter har inletts bland de berörda medlemsstaterna. Utvärderingen ska grundas på de respektive medlemsstaternas rapporter.

2. Närmare uppgifter om förfarandet anges i kapitel 4 i bilagan till detta beslut.

Artikel 22

Förhållandet till genomförandeavtalet till Prümfördraget

För de medlemsstater som är bundna av Prümfördraget ska de tillämpliga bestämmelserna i detta beslut och dess bilaga – så snart de har genomförts fullt ut – tillämpas i stället för motsvarande bestämmelser i genomförandeavtalet till Prümfördraget. Varje annan bestämmelse i Prümfördraget ska fortfarande vara tillämplig mellan de fördragsslutande parterna i Prümfördraget.

Artikel 23

Genomförande

Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att följa bestämmelserna i detta beslut inom de tidsfrister som avses i artikel 36.1 i beslut 2008/615/RIF.

Artikel 24

Tillämpning

Detta beslut får verkan tjugo dagar efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Luxemburg den 23 juni 2008.

På rådets vägnar

I. JARC

Ordförande

BILAGA

INNEHÅLLSFÖRTECKNING

KAPITEL 1: **Utbyte av DNA-uppgifter**

1. ***DNA-relaterade kriminaltekniska frågor, matchningsregler och algoritmer***

1.1 *DNA-profilernas egenskaper*

1.2 *Matchningsregler*

1.3 *Rapporteringsregler*

2. ***Tabell över medlemsstatskoder***

3. ***Funktionsanalys***

3.1 *Systemets tillgänglighet*

3.2 *Steg 2*

4. ***Dokument för gränssnittskontroll – DNA***

4.1 *Inledning*

4.2 *Definition av XML-strukturen*

5. ***Tillämpnings-, säkerhets, och kommunikationsarkitektur***

5.1 *Översikt*

5.2 *Högnivåarkitektur*

5.3 *Säkerhetsstandarder och dataskydd*

5.4 *Protokoll och standarder för krypteringsmekanismen: S/MIME och därmed sammanhörande paket*

5.5 *Tillämpningsarkitektur*

5.6 *Protokoll och standarder för tillämpningsarkitekturen*

5.7 *Kommunikationsmiljö*

KAPITEL 2: **Utbyte av fingeravtrycksuppgifter (gränssnittskontrolldokument)**

1. ***Översikt av filinnehållet***

2. ***Postformat***

3. ***Logisk post typ 1: Filhuvud***

4. ***Logisk post typ 2: Beskrivande text***

5. ***Logisk post typ 4: Högupplösningsbild i gråskala***

6. ***Logisk post typ 9: Minutiaepost***

7. ***Post typ 13: Bilder av latenta avtryck med varierande upplösning***

8. ***Post typ 15: Bilder av handavtryck med varierande upplösning***

9. ***Bilagor till kapitel 2***

9.1 *ASCII-koder för avgränsare*

9.2 *Beräkning av alfanumeriskt kontrolltecken*

9.3 *Teckenkoder*

9.4 *Sammanfattning av transaktioner*

9.5 *Post typ 1 definitioner*

9.6 *Post typ 2 definitioner*

9.7 *Koder för gråskalekomprimering*

9.8 *E-postspecifikation*

KAPITEL 3: **Utbyte av uppgifter i fordonsregister**

1. ***Gemensam uppsättning uppgifter för automatiserad sökning i fordonsregister***

1.1 *Definitioner*

1.2 *Sökning på fordon/ägare/innehavare*

2. ***Datasäkerhet***

2.1 *Översikt*

2.2 *Säkerhetsfunktioner i samband med meddelandeutbytet*

2.3 *Säkerhetsfunktioner utan samband med meddelandeutbytet*

3. ***Tekniska villkor för informationsutbytet***

3.1 *Allmän beskrivning av Eucaris-applikationen*

3.2 *Funktionella och icke funktionella krav*

KAPITEL 4: **Utvärdering**

1. ***Utvärderingsförfarande i enlighet med artikel 20 (förberedelse av beslut enligt artikel 25.2 i beslut 2008/615/RIF)***

1.1 *Frågeformulär*

1.2 *Testkörning*

1.3 *Utvärderingsbesök*

1.4 *Rapport till rådet*

2. ***Utvärderingsförfarande enligt artikel 21***

2.1 *Statistik och rapport*

2.2 *Revidering*

3. ***Expertmöten***

KAPITEL 1: **Utbyte av DNA-uppgifter**

1. ***DNA-relaterade kriminaltekniska frågor, matchningsregler och algoritmer***

1.1 *DNA-profilernas egenskaper*

DNA-profilen kan innehålla 24 talpar som representerar allelerna i 24 lokus som också används vid Interpols DNA-förfaranden. Benämningarna för dessa lokus framgår av följande tabell:

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

De sju gråmarkerade lokusen i den översta raden utgör både den nuvarande europeiska standarduppsättningen av lokus (ESS) och Interpols standarduppsättning av lokus (Issol).

Inklusionsregler:

De DNA-profiler som medlemsstaterna gör tillgängliga för sökning och jämförelse samt de DNA-profiler som sänds för sökning och jämförelse måste innehålla minst 6 fullständigt angivna ([1]) lokus och får innehålla ytterligare lokus eller tomma positioner beroende på tillgång. DNA-personprofiler måste innehålla minst 6 av de 7 ESS-lokusen. För att öka noggrannheten vid matchningen ska alla tillgängliga alleler lagras i den indexerade databasen med DNA-profiler och användas för sökning och jämförelse. Varje medlemsstat ska så snart det är praktiskt möjligt tillämpa varje ny ESS-lokus som antas av EU.

Blandade profiler är inte tillåtna, vilket gör att allel-värdena för varje lokus består av endast två tal. Vid homozygositet kan dessa tal vara lika för ett givet lokus.

Jokertecken och mikrovarianter ska behandlas enligt följande regler:

— Varje icke-numeriskt värde utom amelogenin som profilen innehåller (t.ex. ”o”, ”f”, ”r”, ”na”, ”nr” eller ”un”) måste automatiskt konverteras till ett jokertecken (*) vid exporten och sökas mot alla.

— De numeriska värdena ”0”, ”1” or ”99” i profilen måste automatiskt konverteras till ett jokertecken (*) vid exporten och sökas mot alla.

— Om 3 alleler ges för ett lokus ska den första allelen godtas och de återstående 2 måste automatiskt konverteras till ett jokertecken (*) vid exporten och sökas mot alla.

— Om jokertecken ges för allel 1 eller 2 ska båda permutationerna av det numeriska värdet för lokuset sökas (”12,*” kan till exempel matcha ”12,14” eller ”9,12”).

— Mikrovarianter av pentanukleotider (Penta D, Penta E och CD4) ska matchas på följande sätt:

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

— Mikrovarianter av tetranukleotider (övriga lokus är tetranukleotider) ska matchas på följande sätt:

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

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

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

([1]) ”Fullständigt angivna” betyder att hantering av ovanliga alleler inkluderas.

1.2 *Matchningsregler*

Jämförelsen av två DNA-profiler ska göras på grundval av de lokus för vilka ett par allelvärden är tillgängliga i båda DNA-profilerna. Minst 6 fullständigt angivna lokus (exklusive amelogenin) måste överensstämma mellan de två DNA-profilerna innan ett träffsvar ges.

Full överensstämmelse (*Quality 1*) definieras som en överensstämmelse där samtliga allelvärden är identiska för de jämförda lokus som finns både i den DNA-profil som används för sökningen och i den sökta DNA-profilen. Nära överensstämmelse definieras som en överensstämmelse där värdet för endast en av samtliga jämförda alleler skiljer sig mellan de två DNA-profilerna (*Quality 2, 3* och *4*). En nära överensstämmelse godtas endast om det finns minst 6 fullständigt angivna lokus med full överensstämmelse i de två jämförda DNA-profilerna.

Anledningen till en nära överensstämmelse kan vara

— ett skrivfel vid inmatningen av en av DNA-profilerna i sökningen eller i DNA-databasen,

— ett fel vid allelbestämningen eller allelanropet under förfarandet för generering av DNA-profilen.

1.3 *Rapporteringsregler*

Både fulla överensstämmelser, nära överensstämmelser och ”inga träffar” ska rapporteras.

Överensstämmelserapporten ska sändas till den begärande nationella kontaktpunkten samt göras tillgänglig för den tillfrågade nationella kontaktpunkten (så att den kan uppskatta arten av och antal eventuella uppföljande begäranden om ytterligare personuppgifter och annan information med anknytning till den DNA-profil som svarar mot träffen i enlighet med artiklarna 5 och 10 i beslut 2008/615/RIF).

2. ***Tabell över medlemsstatskoder***

I enlighet med beslut 2008/615/RIF, används ISO 3166-1 tvåställiga bokstavskoder för att upprätta domännamn och andra konfigurationsparametrar som krävs för Prümtillämpningarna för utbyte av DNA-uppgifter via ett slutet nät.

De tvåställiga medlemsstatskoderna enligt ISO 3166-1 alpha-2 är följande:

Medlemsstatens namn	Kod	Medlemsstatens namn	Kod
Belgien	BE	Luxemburg	LU
Bulgarien	BG	Ungern	HU
Tjeckien	CZ	Malta	MT
Danmark	DK	Nederländerna	NL
Tyskland	DE	Österrike	AT
Estland	EE	Polen	PL
Grekland	EL	Portugal	PT
Spanien	ES	Rumänien	RO
Frankrike	FR	Slovakien	SK
Irland	IE	Slovenien	SI
Italien	IT	Finland	FI
Cypern	CY	Sverige	SE
Lettland	LV	Förenade kungariket	UK
Litauen	LT		

3. ***Funktionsanalys***

3.1 *Systemets tillgänglighet*

En begäran om sökning enligt artikel 3 i beslut 2008/615/RIF bör nå den anropade databasen i kronologisk ankomstordning enligt vilken begäran sändes, medan svaren bör nå den anmodande medlemsstaten inom 15 minuter efter det att begäran inkom.

3.2 *Steg 2*

När en medlemsstat mottar en rapport om överensstämmelse ansvarar den nationella kontaktpunkten för en jämförelse mellan värdena i den profil som sänds som fråga och värdena i den profil/de profiler som har mottagits som svar i syfte att validera och kontrollera profilens bevisvärde. De nationella kontaktpunkterna kan ta direktkontakter i valideringssyfte.

Förfaranden för rättslig hjälp inleds efter det att en överensstämmelse mellan två profiler validerats, på grundval av ”fullständig överensstämmelse” eller ”nära överensstämmelse” under det automatiska sökningsförfarandet.

4. ***Dokument för gränssnittskontroll – DNA***

4.1 *Inledning*

4.1.1 Syfte

Detta kapitel anger kraven för informationsutbytet om DNA-profiler mellan samtliga medlemsstaters DNA-databassystem. Fälten i huvudet är specificerade speciellt för Prüm-utbytet av DNA-uppgifter och datadelen grundar sig på datadelen för DNA-uppgifter enligt XML-schemat för Interpols nätport för utbyte av DNA-uppgifter.

Uppgifterna utbyts genom SMTP (Simple Mail Transfer Protocol) med användning av en central e-postserver som ställs till förfogande av nätoperatören. XML-filen överförs som meddelandetext.

4.1.2 Omfattning

Detta dokument för gränssnittskontroll, ICD, rör endast e-postmeddelandets innehåll. Alla nätspecifika och e-postspecifika områden definieras på ett likartat sätt för att ge en gemensam teknisk grund för utbytet av DNA-uppgifter.

Detta inbegriper

— formatet för meddelandets ärendefält, så att meddelandena kan bearbetas automatiskt,

— specifikationer av huruvida kryptering erfordras och i så fall vilka metoder som bör väljas,

— maximilängd för meddelandena.

4.1.3 XML-struktur och XML-principer

XML-meddelandet är indelat i

— ett huvud som innehåller information om överföringen, och

— en datadel som innehåller profilspecifik information samt själva profilen.

Samma XML-schema ska kunna användas för både begäran och svar.

För fullständiga kontroller av oidentifierade DNA-profiler (artikel 4 i beslut 2008/615/RIF) ska det vara möjligt att sända en uppsättning profiler i ett enda meddelande. Det maximala antalet profiler i ett meddelande måste fastställas. Detta antal är beroende av den maximala meddelandestorleken och ska fastställas efter val av e-postserver.

XML-exempel:

<?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> datastrukturen upprepas om fler än en profil sänds i (....) ett enda SMTP-meddelande, något som endast tillåts i fall enligt artikel 4

</datas>

</PRUEMDNA>

4.2 *Definition av XML-strukturen*

Följande definitioner medtas endast i dokumentationssyfte och för bättre läsbarhet, den faktiskt bindande informationen återfinns i en fil med XML-schemat (PRUEM DNA.xsd).

4.2.1 Specifikation PRUEMDNAx

Den innehåller följande fält:

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

4.2.2 Innehåll i huvudfältets struktur

4.2.2.1 PRUEM-huvud

Denna struktur beskriver XML-filhuvudet. Den innehåller följande fält:

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

4.2.2.2 PRUEM_header dir

Typ av data i meddelandet, värden

Value	Description
R	Request

Value	Description
A	Answer

4.2.2.3 Information i PRUEM-huvudet

Struktur som beskriver medlemsstaten samt anger datum och tid för meddelandet. Den innehåller följande fält:

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

4.2.3 PRUEM-profiluppgifter, innehåll

4.2.3.1 PRUEM_datas

Denna struktur beskriver XML-profilens datadel: Den innehåller följande fält:

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

4.2.3.2 PRUEM_request_type

Typ av data i meddelandet, värden:

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

4.2.3.3 PRUEM_hitquality_type

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

4.2.3.4 PRUEM_data_type

Typ av data i meddelandet, värden:

Value	Description
P	Person profile
S	Stain

4.2.3.5 PRUEM_data_result

Typ av data i meddelandet, värden:

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

4.2.3.6 IPSG_DNA_profile

Struktur som beskriver en DNA-profil. Den innehåller följande fält:

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

4.2.3.7 IPSG_DNA_ISSOL

Struktur som innehåller Issol-lokus (Interpols standarduppsättning lokus). Den innehåller följande fält:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

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

4.2.3.8 IPSG_DNA_additional_loci

Struktur som innehåller övriga lokus. Den innehåller följande fält:

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

4.2.3.9 IPSG_DNA_locus

Struktur som beskriver ett lokus. Den innehåller följande fält:

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

5. *Tillämpnings-, säkerhets- och kommunikationsarkitektur*

5.1 *Översikt*

Vid införandet av tillämpningar för utbyte av DNA-uppgifter inom ramen för beslut 2008/615/RIF ska ett gemensamt, på logisk nivå slutet, nät mellan medlemsstaterna användas. För att mer effektivt utnyttja detta

gemensamma kommunikationsnät för att sända begäranden och ta emot svar ska begäranden om DNA- och fingeravtrycksuppgifter överföras asynkront i inkapslade SMTP-meddelanden. Av hänsyn till säkerhetskraven kommer S/MIME-mekanismen att användas som tillägg till SMTP-funktionerna för att upprätta en obruten säker tunnel i nätet.

Det redan fungerande systemet Testa (Trans European Services for Telematics between Administrations) har valts som kommunikationsnät för datautbytet mellan medlemsstaterna. Europeiska kommissionen ansvarar för närvarande för Testa. Eftersom de nationella DNA-databaserna och de nuvarande nationella anslutningspunkterna för Testa kan vara belägna på olika ställen i medlemsstaterna kan tillgång till Testa anordnas antingen

1) genom att använda den befintliga nationella anslutningspunkten eller inrätta en ny nationell anslutningspunkt till Testa, eller

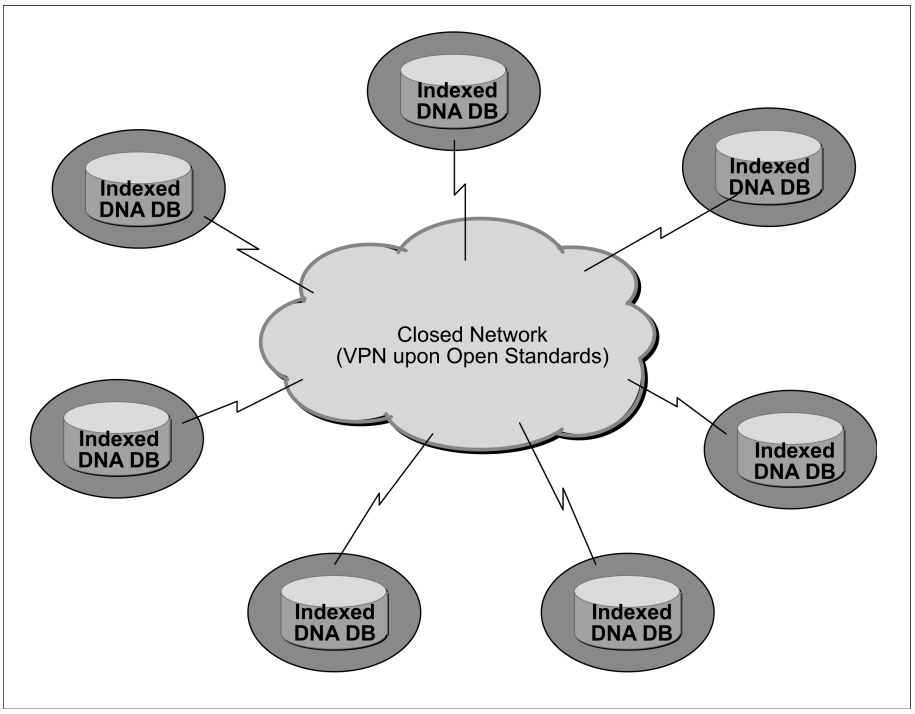
2) genom att etablera en säker lokal länk, från den plats där DNA-databasen finns och förvaltas av det behöriga nationella organet, till den befintliga nationella anslutningspunkten till Testa.

De protokoll och standarder som används vid införandet av tillämpningar enligt beslut 2008/615/RIF står i överensstämmelse med öppna standarder och uppfyller de kraven från dem som ansvarar för medlemsstaternas nationella säkerhet.

5.2 *Högnivåarkitektur*

Enligt beslut 2008/615/RIF ska varje medlemsstat göra sin DNA-databas tillgänglig för utbyte med och/eller sökning från andra medlemsstater i enlighet med ett standardiserat gemensamt dataformat. Arkitekturen bygger på kommunikationsmodellen alla-till-alla (*any-to-any*). Det finns ingen central server och inte heller någon centraliserad databas med DNA-profiler.

Figur 1: Topologi över utbyte av DNA-uppgifter



Medlemsstaterna ska iaktta de nationella rättsliga restriktionerna för medlemsstaternas webbplatser och kan också bestämma vilken typ av hårdvara och vilka program som bör användas för att konfigurera medlemsstatens webbplats för att iaktta kraven i beslut 2008/615/RIF.

5.3 *Säkerhetsstandarder och dataskydd*

Tre nivåer av säkerhetsklassning har övervägts och införts.

5.3.1 Datanivån

De DNA-profiluppgifter som tillhandahålls av varje medlemsstat måste utformas i enlighet med en gemensam standard för dataskydd så att den begärande medlemsstaten får ett svar som huvudsakligen anger TRÄFF eller ICKE-TRÄFF samt vid TRÄFF ett identifikationsnummer som inte innehåller några som helst personuppgifter. Den fortsatta undersökningen efter meddelande om TRÄFF kommer att genomföras på bilateral nivå i enlighet med de nationella rättsliga och organisatoriska föreskrifter som gäller vid respektive medlemsstats anläggning.

5.3.2 Kommunikationsnivån

Meddelanden som innehåller information om DNA-profiler (begäranden och svar) kommer att krypteras med senaste teknik, anpassad till öppna standarder, t.ex. S/MIME, innan de översänds till andra medlemsstaters anläggningar.

5.3.3 Transmissionsnivån

Alla krypterade meddelanden med DNA-profilinformation kommer att vidarebefordras till andra medlemsstaters anläggningar genom ett virtuellt privat tunnelsystem som på internationell nivå förvaltas av en tillförlitlig nätleverantör och med nationellt ansvar för de säkra länkarna till detta tunnelsystem. Det virtuella privata tunnelsystemet har ingen anslutning till det öppna Internet.

5.4 *Protokoll och standarder för krypteringsmekanismen S/MIME och därmed sammanhörande paket*

Den öppna standarden S/MIME, en vidareutveckling av den faktiska e-poststandarden SMTP, kommer att användas för att kryptera meddelanden med DNA-profilinformation. Protokollet S/MIME (version 3) ger möjlighet till signerade kvittenser, säkerhetsuppmärkning och säkra sändlistor på grundval av en kryptografisk meddelandestandard (*Cryptographic Message Syntax,* CMS), en specifikation från *Internet Engineering Task Force* (IETF) för meddelanden skyddade genom kryptering. Det kan användas för att digitalt signera, autentisera eller kryptera alla former av uppgifter i digital form.

Det certifikat som S/MIME-mekanismen använder måste överensstämma med X.509-standarden. För att se till att de gemensamma standarderna och förfarandena överensstämmer med andra Prüm-tillämpningar gäller följande regler för S/MIME-kryptering eller i samband med olika Cots-miljöer (Cots, färdigköpt allmänt tillgänglig produkt).

— Bearbetningsordning: Först kryptering, därefter signering.

— Krypteringsalgoritmerna AES (*Advanced Encryption Standard*) med 256 bitars nyckellängd och RSA med 1 024 bitars nyckellängd ska användas för symmetrisk respektive asymmetrisk kryptering.

— Hash-algoritmen SHA-1 ska användas.

S/MIME-funktioner finns i de allra flesta moderna programpaket för e-post, bland annat Outlook, Mozilla Mail och Netscape Communicator 4.x och är interoperabla mellan alla viktigare programpaket för e-post.

S/MIME har valts som lämplig mekanism för dataskyddet på kommunikationsnivån eftersom den är lätt att införliva i den nationella infrastrukturen vid alla medlemsstaters anläggningar. För att på ett effektivare sätt och till lägre kostnader visa hur tekniken fungerar har dock den öppna standarden JavaMail API valts för prototypen till utbytet av DNA-uppgifter. JavaMail API erbjuder enkel kryptering och dekryptering av e-postmeddelanden med användning av S/MIME och/eller OpenPGP. Avsikten är att erbjuda ett enkelt och lättanvänt API för e-postkunder som vill sända och ta emot e-post i något av de två mest populära formaten för krypterade e-postmeddelanden. Därför är det tillräckligt med någon av de senaste tillämpningarna av *JavaMail API* för de krav som ställs i beslut 2008/615/RIF, t.ex. en produkt från *Bouncy Castle JCE (Java Cryptographic Extension)*, som kommer att användas för tillämpningen av S/MIME för prototypen av utbytet av DNA-uppgifter mellan alla medlemsstater.

5.5 *Tillämpningsarkitektur*

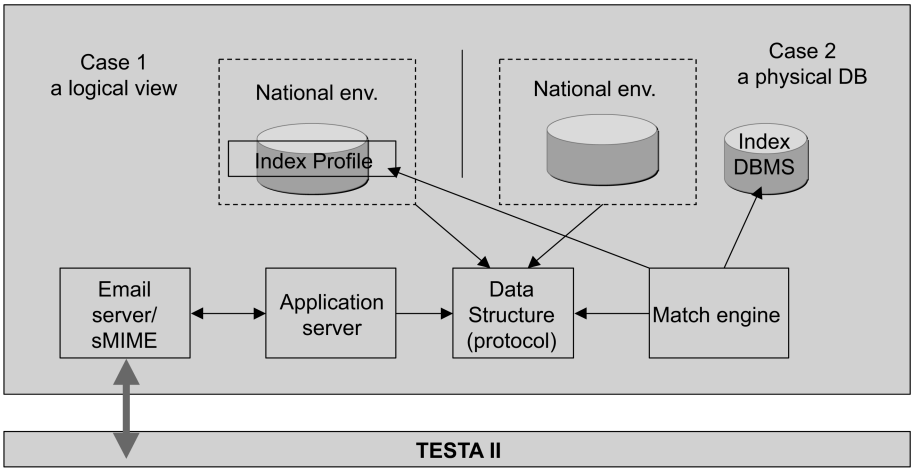
Varje medlemsstat kommer att ge övriga medlemsstater en uppsättning standardiserade DNA-profiluppgifter som är anpassade till gällande dokument för gränssnittskontroll (*Interface Control Document, ICD*). Detta kan antingen göras genom en logisk visning av den enskilda nationella databasen eller genom att upprätta en fysiskt exporterad databas (indexerad databas).

De fyra huvuddelarna: E-postservern/S/MIME, tillämpningsservern, datastrukturområdet för hämtning/inmatning av uppgifter och registrering av inkommande/utgående meddelanden samt matchningsmotorn genomför tillämpningslogiken på ett produktoberoende sätt.

För att alla medlemsstater lätt ska kunna införliva dessa komponenter i sina respektive anläggningar har de specificerade gemensamma funktionerna införts genom öppna standarder och protokoll som varje medlemsstat själv kan välja med hänsyn till nationell IT-policy och nationella IT-föreskrifter. På grund av de oberoende funktioner som ska införas för att få tillgång till de indexerade DNA-profildatabaser som omfattas av beslut 2008/615/RIF kan varje medlemsstat fritt välja plattform för hårdvara och program, inklusive databas- och operativsystem.

En prototyp för utbytet av DNA-uppgifter har utarbetats och prövats med framgång på det befintliga gemensamma nätet. Version 1.0 har utnyttjats i produktionsmiljö och används för det löpande arbetet. Medlemsstaterna får använda den produkt som har utvecklats gemensamt men får också utveckla egna produkter. De gemensamma produktkomponenterna kommer att bevaras, anpassas och vidareutvecklas i enlighet med de förändrade kraven inom IT, kriminaltekniken och/eller polisfunktionerna.

Figur 2: Översikt av tillämpningstopologin



5.6 *Protokoll och standarder för tillämpningsarkitekturen*

5.6.1 XML

Vid utbytet av DNA-uppgifter kommer XML-schemat, som bifogas e-postmeddelanden enligt SMTP, att användas fullt ut. XML (Xtensible Markup Language) är ett av W3C rekommenderat allmänt markeringsspråk för att för särskilda ändamål skapa markeringsspråk som kan beskriva många olika former av uppgifter. En beskrivning av en DNA-profil som lämpar sig för utbyte mellan alla medlemsstater har utarbetats med hjälp av XML och XML-schemat i dokumentet för gränssnittskontroll.

5.6.2 ODBC

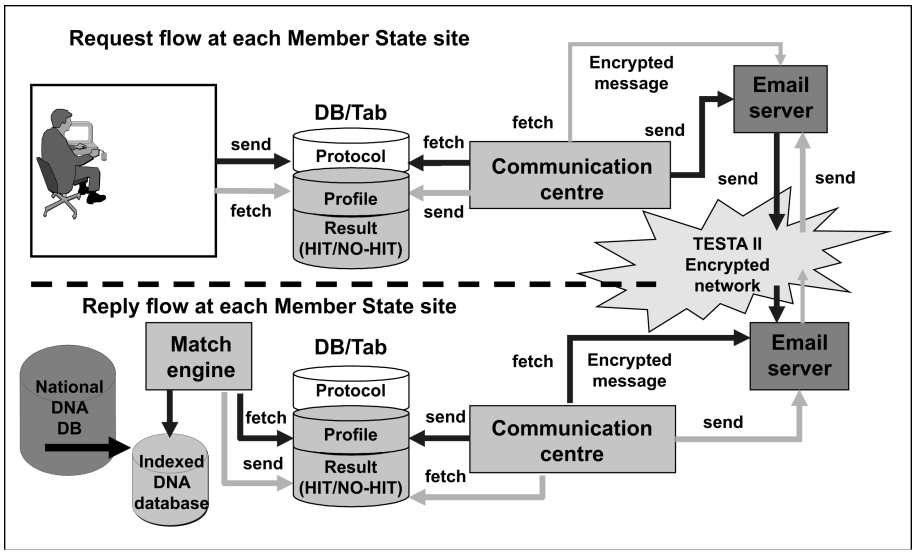
Open DataBase Connectivity tillhandahåller ett standardiserat programmeringsgränssnitt (*Application Program Interface, API*) som ger åtkomst till databashanterare, oberoende av programmeringsspråk, databassystem och operativsystem. ODBC har dock vissa nackdelar. Att hantera ett stort antal klienter kan innebära en mångfald drivrutiner och dynamiska länkbibliotek (DLL). Dessa komplikationer kan öka omkostnaderna för administration av systemet.

5.6.3 JDBC

Java DataBase Connectivity (JDBC) är ett programgränssnitt (API) for programmeringsspråket Java som definierar på vilket sätt en klient kan ha åtkomst till en databas. I motsats till *ODBC* kräver inte *JDBC* några särskilda DLL i den lokala persondatorn.

Affärslogiken för att bearbeta begäran om DNA-profiler och svar på dessa vid medlemsstaternas anläggningar beskrivs i följande diagram. Både flödet för begäran och flödet för svar växelverkar med ett neutralt dataområde bestående av olika datapooler med gemensam datastruktur.

Figur 3: Tillämpningens arbetsflöde vid medlemsstaternas anläggningar, översikt



5.7 *Kommunikationsmiljö*

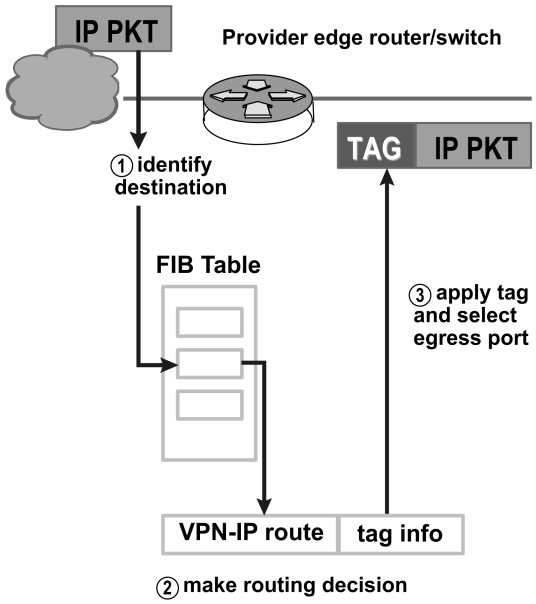
5.7.1 Gemensamt kommunikationsnät: Testa och efterföljande infrastruktur

Tillämpningen för utbyte av DNA-uppgifter kommer att använda e-post, en asynkron mekanism, för att begära sökningar och ta emot svar mellan medlemsstaterna. Eftersom alla medlemsstater har minst en nationell anslutningspunkt till Testa-nätet kommer det nätet att användas för utbytet av DNA-uppgifter. Testa tillhandahåller ett antal mervärdestjänster via sitt e-postrelä. Infrastrukturen fungerar som värd för Testa-specifika e-postlådor och kan dessutom omfatta sändlistor och policy för dirigering. Detta gör att Testa kan användas som en clearingcentral för meddelanden som är adresserade till förvaltningar som är anslutna till EU-omfattande domäner. Mekanismer för viruskontroll kan också inrättas.

Relästationen för e-post i Testa är byggd på en maskinvaruplattform med hög tillgänglighet vid den centrala Testa-anläggningen och skyddas av en brandvägg. DNS-servern i Testa konverterar URL-strängar till IP-adresser så att adresseringsfrågorna inte berör användare och tillämpningar.

5.7.2 Säkerhetsfrågan

VPN-konceptet (Virtuellt Privat Nät) är genomfört inom ramen för Testa. Den teknik för *Tag Switching* som används för att bygga upp detta VPN kommer att utvecklas så att den är anpassad för den standard för *MPLS (Multi-Protocol Label Switching)* som har utarbetats av *IETF (Internet Engineering Task Force)*.



MPLS är en standardteknik från IETF som påskyndar trafikflödet i nätet genom att inte analysera paketen i mellanliggande routrar (”hops”). Detta görs med hjälp av s.k. etiketter som bifogas paketet av stamnätets gränsroutrar på grundval av information i *FIB (Forwarding Information Base)*. Etiketter används också för att genomföra virtuella privata nät.

MPLS kombinerar fördelarna med lager 3-routning och lager 2-switchning. Eftersom IP-adresserna inte analyseras vid överföringen i stamnätet, medför MPLS inte några begränsningar vad gäller IP-adresseringen.

Dessutom kommer e-postmeddelanden i Testa att skyddas av en krypteringsmekanism driven av S/MIME. Utan kännedom om nyckeln och utan rätt certifikat är det omöjligt att dekryptera meddelanden som sänds via nätet.

5.7.3 Protokoll och standarder för kommunikationsnätet

5.7.3.1 SMTP

SMTP *(Simple Mail Transfer Protocol)* är en de facto-standard för överföring av e-post via Internet. SMTP är ett relativt enkelt textbaserat protokoll där man anger en eller flera mottagare och därefter överför meddelandetexten. SMTP använder TCP-port 25 enligt IETF:s specifikation. För att hitta SMTP-servern för en visst domännamn används DNS-informationen vid MX (Mail eXchange).

Eftersom detta protokoll till att börja med uteslutande grundade sig på ASCII-text, kunde det inte hantera binära filer särskilt bra. Standarder som MIME utarbetades för att koda binära filer för överföring med SMTP. Numera är de flesta SMTP-servrarna anpassade till vidareutvecklingarna 8BITMIME och S/MIME, vilket gör att binära filer kan överföras nästan lika enkelt som klartext. Bearbetningsreglerna för S/MIME beskrivs i S/MIME-avsnittet.

SMTP är ett push-protokoll som gör att meddelanden inte kan hämtas från en fjärrserver på begäran. För att göra detta måste postkunden använda POP3 eller IMAP. Man har beslutat att använda POP3-protokollet för utbytet av DNA-uppgifter.

5.7.3.2 POP

De lokala e-postkunderna använder protokollet POP3 (*Post Office Protocol, version 3*), ett Internet-standardprotokoll för tillämpningslagret, för att hämta e-post från en fjärrserver via en TCP/IP-förbindelse. Genom att använda SMTP-protokollets profil för ”skicka” sänder e-postkunder meddelanden över Internet eller över ett företagsinternt nät. MIME används som standard för bilagor och icke-ASCII-text. Även om varken POP3 eller SMTP kräver MIME-formaterad e-post, kommer så gott som all e-post via Internet i MIME-format, vilket innebär att även POP-klienterna måste förstå och använda MIME. Hela kommunikationsmiljön enligt beslut 2008/615/RIF kommer därför att inkludera POP-komponenterna.

5.7.4 Tilldelning av nätadresser

Driftsmiljö

Testa har av den europeiska IP-registreringsmyndigheten (RIPE) redan tilldelats ett särskilt block av subnet-adresser av klass C. Ytterligare block av adresser kan senare komma att tilldelas Testa vid behov. Tilldelningen av IP-adresser till medlemsstaterna grundar sig på ett geografiskt mönster i Europa. Uppgiftsutbytet mellan medlemsstaterna inom ramen för beslut 2008/615/RIF genomförs i ett logiskt slutet IP-nät som omfattar hela Europa.

Testmiljö

För att tillhandahålla en väl fungerande miljö för den dagliga verksamheten i alla anslutna medlemsstater måste en testmiljö upprättas i det slutna nätet för nya medlemsstater som förbereder sitt deltagande. Ett blad med parametrar, bland annat IP-adresser, nätinställningar, e-postdomäner och användarkonton för tillämpningen har utarbetats och bör anslås vid dessa medlemsstaters anläggningar. En uppsättning pseudo-DNA-profiler för teständamål har också utformats.

5.7.5 Konfigurationsparametrar

Ett säkert e-postsystem har upprättats med användning av domänen eu-admin.net. Denna domän kommer inte att kunna nås från en plats som inte ingår i den EU-omfattande Testa-domänen, eftersom namnen endast är kända på Testas centrala DNS-server, som är skyddad från Internet.

Mappningen av dessa webbplatsadresser (värdnamn) till motsvarande IP-adresser sköts genom DNS-tjänsten i Testa. För varje lokal domän kommer ett postobjekt att läggas till på Testas centrala DNS-server, varifrån alla e-postmeddelanden från Testas lokala domäner skickas vidare till Testas centrala postrelä. Det centrala postrelät kommer därefter att vidarebefordra dem till den specifika lokala domänens e-postserver och använda de lokala domänernas e-postadresser. Genom att skicka vidare e-posten på detta sätt kommer kritisk information i e-postmeddelandena endast att passera den EU-omfattande slutna nätinfrastrukturen, inte det osäkra Internet.

Subdomäner (***fet kursiv stil***) enligt följande syntax måste upprättas för alla medlemsstaters anläggningar:

"***typ_av_tillämpning*.pruem.*medlemsstatskod*.*eu-admin*.*net***", där

värdet för "***medlemsstatskod***" är en av de tvåställiga bokstavskoderna för medlemsstaterna (dvs. "AT", "BE" etc.), och

värdet för "***typ_av_tillämpning***" är antingen DNA eller FP.

Med denna syntax blir medlemsstaternas subdomäner följande:

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

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

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

KAPITEL 2: **Utbyte av fingeravtrycksuppgifter (gränssnittskontrolldokument)**

Syftet med följande gränssnittskontrolldokument är att fastställa kraven för utbytet av fingeravtrycksuppgifter mellan AFIS-systemen i medlemsstaterna (Automated Fingerprint Identification Systems). Det grundar sig på Interpols implementation av ANSI/NIST-ITL 1-2000 (INT-I, version 4.22b).

Denna version ska omfatta alla grundläggande definitioner för de logiska posterna av typ 1, typ 2, typ 4, typ 9, typ 13 och typ 15 som krävs för bearbetning av fingeravtrycken utgående från bilder och minutiae.

1. ***Översikt av filinnehållet***

En fingeravtrycksfil består av flera logiska poster. I den ursprungliga standarden ANSI/NIST-ITL 1-2000 specificeras 16 posttyper. Lämpliga ASCII-avgränsare sätts in mellan posterna och mellan fält och delfält i posterna.

Endast sex posttyper används för att utbyta uppgifter mellan det sändande och det mottagande organet.

Typ 1 → Transaktionsinformation

Typ 2 → Alfanumeriska person- och/eller ärendeuppgifter

Typ 4 → Högupplösta fingeravtrycksbilder i gråskala

Typ 9 → Minutiaepost

Typ 13 → Post för latent bild med varierande upplösning

Typ 15 → Post för handavtrycksbild med varierande upplösning

1.1 *Typ 1 – Filhuvud*

Denna post innehåller routningsinformation och information som beskriver strukturen i resten av filen. Denna posttyp definierar också transaktionstypen, som ingår i någon av följande övergripande kategorier:

1.2 *Typ 2 – Beskrivande text*

Denna post innehåller informerande text av intresse för det sändande och det mottagande organet.

1.3 *Typ 4 – Högupplöst bild i gråskala*

Denna post används för att utbyta högupplösta fingeravtrycksbilder i gråskala (8 bitar) som skannats med upplösningen 500 pixel/tum. Fingeravtrycksbilderna ska komprimeras med WSQ-algoritmen i ett förhållande som inte överstiger 15:1. Andra komprimeringsalgoritmer eller okomprimerade bilder får inte användas.

1.4 *Typ 9 – Minutiaepost*

Posttyp 9 används för att utbyta karakteristiska papillarmönster eller uppgifter om minutiae. De tjänar dels till undvika onödig dubblering av AFIS-kodningsprocesserna, dels till att göra det möjligt att överföra AFIS-koder som innehåller färre uppgifter än motsvarande bilder.

1.5 *Typ 13 – Latenta bilder med varierande upplösning*

Denna post ska användas för att utbyta bilder av latenta fingeravtryck och handavtryck tillsammans med alfanumerisk textinformation. Bilder ska vara skannade med upplösningen 500 pixel/tum i 256 nivåer av grått. Om den latenta bildens kvalitet tillåter det, ska den komprimeras med WSQ-algoritmen. Om så behövs får, efter ömsesidig överenskommelse, bildernas upplösning ökas så att den överskrider 500 pixel/tum och gråskalan utvidgas till fler än 256 nivåer. I detta fall bör man absolut använda JPEG 2000 (se bilaga 7).

1.6 *Post för handavtrycksbild med varierande upplösning*

Poster av typ 15 med taggade fält ska användas för att utbyta handavtrycksbilder med varierande upplösning tillsammans med alfanumerisk textinformation. Bilder ska vara skannade med upplösningen 500 pixel/tum i 256 nivåer av grått. För att minimera datamängderna ska alla handavtrycksbilder komprimeras med WSQ-mekanismen. Om så behövs får, efter ömsesidig överenskommelse, bildernas upplösning ökas så att den överskrider 500 pixel/tum och gråskalan utvidgas till fler än 256 nivåer. I detta fall bör man absolut använda JPEG 2000 (se bilaga 7).

2. ***Postformat***

En transaktionsfil ska bestå av en eller flera logiska poster. I varje logisk post i filen ska det finnas flera fält med information associerad med posttypen i fråga. Varje informationsfält kan innehålla en eller flera grundläggande uppgifter som var och en representeras av endast ett värde. Sammantagna används dessa uppgifter för att förmedla olika aspekter av informationen i fältet. Ett informationsfält kan också bestå av en eller flera grupperade uppgifter som upprepas flera gånger inom fältet. En sådan grupp av uppgifter kallas delfält. Ett informationsfält kan därför bestå av ett eller delfält med uppgifter.

2.1 *Informationsavgränsare*

I de logiska posterna med taggade fält skiljs de olika informationskomponenterna från varandra med hjälp av fyra informationsavgränsare i ASCII-kod. De på så sätt avgränsade informationskomponenterna kan vara uppgifter inom ett fält eller ett delfält, fält i en logisk post eller de olika förekomsterna av delfält. Dessa informationsavgränsare definieras i ANSI X3.4-standarden. Dessa tecken används för att avgränsa och kvalificera information i logisk mening. Sedda i hierarkisk ordning uppifrån och ner är filavgränsningstecknet ”FS” den mest inklusiva avgränsaren, följd av gruppavgränsaren ”GS”, postavgränsaren ”RS” och sist enhetsavgränsningstecknet ”US”. Dessa ASCII-avgränsare, och hur de används inom ramen för denna standard, beskrivs i tabell 1.

Informationsavgränsarna bör ur funktionell synpunkt ses som en anvisning om vilken typ av information som följer efter avgränsaren. US-tecknet ska avgränsa olika enskilda uppgifter inom ett fält eller ett delfält. Det är en signal om att nästa uppgift är en informationskomponent inom det fältet eller delfältet. Flera olika delfält inom ett fält avgränsade med RS-tecknet signalerar början av nästa grupp av upprepade uppgifter. Avgränsningstecknet GS mellan informationsfält signalerar början av ett nytt fält och ska föregå det fältidentifikationsnummer som ska finnas. På liknande sätt ska början av en ny logisk post signaleras av FS-tecknet.

De fyra tecknen är endast meningsfulla när de används som avgränsare av informationskomponenter i fält i poster med ASCII-text. Dessa tecken har ingen särskild betydelse när de förekommer i binära bildposter och binära fält – de ingår då endast i de utbytta uppgifterna.

Det ska normalt inte finnas tomma fält eller uppgifter, och därför bör det endast förekomma ett avgränsningstecken mellan två uppgifter. Undantaget från denna regel inträffar till exempel när data i ett fält eller uppgifter i en transaktion inte är tillgängliga, saknas eller är frivilliga, och bearbetningen av transaktionen inte är beroende av att dessa specifika data finns att tillgå. I dessa fall ska flera och angränsande avgränsningstecken förekomma tillsammans, snarare än att uppgifter utan betydelse infogas mellan avgränsningstecknen.

Följande gäller för definitionen av ett fält som består av tre uppgifter. Om information för den andra uppgiften saknas, kommer två angränsande US-avgränsare att förekomma mellan den första och den tredje uppgiften. Om både den andra och den tredje uppgiften saknades, skulle tre avgränsningstecken användas – två US-tecken förutom den avslutande fält- eller delfältsavgränsaren. Allmänt sett gäller att om en eller flera obligatoriska eller frivilliga uppgifter inte finns att tillgå för ett fält eller ett delfält, ska det relevanta antalet avgränsningstecken infogas.

Det är möjligt att ha kombinationer med två eller flera av de fyra tillgängliga avgränsningstecknen gränsande till varandra. Om data saknas eller inte finns att tillgå för uppgifter, delfält eller fält, måste det förekomma ett avgränsningstecken mindre än antalet erforderliga uppgifter, delfält eller fält.

Tabell 1: Använda avgränsare

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2 *Postformat*

I logiska poster med taggade fält ska varje informationsfält som används numreras i enlighet med följande standard. Varje fält ska formateras så att det består av typnummer för den logiska posten följt av punkt ".", ett fältnummer följt av kolon ":", följt av den för detta fält relevanta informationen. Fältnumret för det taggade fältet kan vara ett godtyckligt en- till niosiffrigt nummer som förekommer mellan punkt "." och kolon ":". Det ska tolkas som ett fältnummer i positivt heltal. Detta innebär att ett fältnummer "2 123:" är lika med och ska tolkas på samma sätt som ett fältnummer "2.000000123:".

I exemplifierande syfte används i hela detta dokument ett treställigt tal för numrering av de fält som ingår de logiska poster med taggade fält som beskrivs i dokumentet. Fältnummer får formatet "TT.xxx:" där "TT" representerar posttypen med ett eller två tecken följt av en punkt. De följande tre tecknen innehåller det relevanta fältnumret som följs av ett kolon. Efter kolon följer ASCII-information eller bilddata.

Logiska poster av typ 1 eller typ 2 innehåller endast datafält med ASCII-text. Den totala postlängden (inklusive fältnummer, kolon och avgränsningstecken) ska anges i det första ASCII-fältet i båda dessa posttyper. ASCII-filavgränsaren "FS" (anger slutet av den logiska posten eller transaktionen) ska följa efter den sista positionen ASCII-information och inkluderas i postlängden.

I motsats till konceptet med taggade fält innehåller poster av typ 4 endast binära data som registrerats i form av ordnade binära fält med fast längd. Den totala postlängden ska anges i det första fältet om fyra positioner i varje post. I denna binära post ska varken postnumret med sin efterföljande punkt eller fältnumret med efterföljande kolon anges. Eftersom alla fältlängder i denna posttyp antingen är fasta eller specificerade, ska inget av de fyra avgränsningstecknen ("US", "RS", "GS", eller "FS") tolkas som någonting annat än binära data. FS-tecknet ska inte användas som post- eller transaktionsavgränsare i den binära posten.

3. ***Logisk post typ 1: Filhuvud***

Denna post beskriver filens struktur och typ samt innehåller annan viktig information. De tecken som används för fält i logiska poster av typ 1 ska endast utgöras av den 7-bitars ANSI-koden för informationsutbyte.

3.1 *Fält i logisk post typ 1*

3.1.1 Fält 1.001: Logisk postlängd (*Logical Record Length – LEN*)

I detta fält anges det totala antalet byte i hela den logiska posten av typ 1. Fältet inleds med "1 001:" följt av den totala postlängden, inklusive alla tecken i alla fält och informationsavgränsarna.

3.1.2 Fält 1.002: Versionsnummer (*Version number – VER*)

För att säkerställa att användarna känner till vilken version av ANSI/NIST-standarden som används, anges i detta fält versionsnumret för den standard som används av det program eller system som har skapat filen. I de första två positionerna anges versionsnumret, i de två följande revisionsnumret. Den ursprungliga standarden från 1986 skulle till exempel anses som den första versionen och anges som ”0100”, medan den nuvarande standarden ANSI/NIST-ITL 1-2000 anges som ”0300”.

3.1.3 Fält 1.002: Fältinnehåll (File Content – CNT)

I detta fält förtecknas varje post i filen efter posttyp och i den ordning i vilken de förekommer i den logiska filen. Det består av ett eller flera delfält, som vart och ett i sin tur innehåller två uppgifter som beskriver en logisk post som förekommer i den aktuella filen. Delfälten registreras i samma ordning som den i vilken posterna registreras och överförs.

Den första uppgiften i det första delfältet är ”1”, vilket hänvisar till denna post av typ 1. Den följs av en andra uppgift om antalet andra poster som förekommer i filen. Detta antal är också lika med antal återstående delfält i fält 1.003.

Vart och ett av de återstående delfälten är förknippat med en post i filen och sekvensen av delfält svarar mot sekvensen av poster. Varje delfält innehåller två uppgifter. Den första uppgiften identifierar posttypen. Den andra uppgiften är postens IDC. US-tecknet ska användas för att avgränsa de två uppgifterna.

3.1.4 Fält 1.003: Transaktionstyp (*Type of Transaction – TOT*)

Detta fält innehåller en treställig minneskod som anger transaktionstypen. Dessa koder kan skilja sig från dem som används i andra implementationer av ANSI/NIST-standarden.

CPS: Criminal Print-to-Print Search. Transaktionen är en begäran om sökning med en post i anslutning till ett brott mot en avtrycksdatabas. Personens avtryck måste inkluderas i filen som WSQ-komprimerade bilder.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1–14 poster typ 4.

Transaktionstypen CPS sammanfattas i tabell A.6.1 (bilaga 6).

PMS: Print-to-Latent Search. Denna transaktion används när en uppsättning avtryck ska användas för sökning mot en databas med oidentifierade latenta avtryck. Svaret kommer att innehålla Träff/Icke-träff-avgörandet vid den avsedda AFIS-sökningen. Om det finns flera oidentifierade latenta avtryck, kommer flera SRE-transaktioner att returneras med ett latent avtryck per transaktion. Personens avtryck måste inkluderas i filen som WSQ-komprimerade bilder.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1 post typ 13.

Transaktionstypen PMS sammanfattas i tabell A.6.1 (bilaga 6).

MPS: Latent-to-Print Search. Denna transaktion används när ett latent avtryck ska användas för sökning mot en avtrycksdatabas. Den latenta minutiaeinformationen och bilden (WSQ-komprimerad) måste ingå i filen.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1 post typ 4 eller typ 15.

Transaktionstypen MPS sammanfattas i tabell A.6.4 (bilaga 6).

MMS: Latent-to-Latent Search. För denna transaktion innehåller filen ett latent avtryck som ska användas för sökning mot en databas med oidentifierade latenta avtryck i syfte att ta konstatera kopplingar mellan olika brottsplatser. Den latenta minutiaeinformationen och bilden (WSQ-komprimerad) måste ingå i filen.

Vid Icke-TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

Vid TRÄFF kommer följande logiska poster att returneras:

— 1 post typ 1.

— 1 post typ 2.

— 1 post typ 13.

Transaktionstypen MMS sammanfattas i tabell A.6.4 (bilaga 6).

SRE: Denna transaktion returneras av bestämmelseorganet som svar på begäran om fingeravtrycksundersökningar. Svaret kommer att innehålla Träff/Icke-träff-avgörandet vid den avsedda AFIS-sökningen. Om det finns flera kandidater, kommer flera SRE-transaktioner att returneras med en kandidat per transaktion.

Transaktionstypen SRE sammanfattas i tabell A.6.2 (bilaga 6).

ERR: Denna transaktion returneras av det avsedda AFIS-systemet för att ange ett fel vid bearbetningen av transaktionen. Den innehåller ett meddelandefält (ERM) som anger vilket fel som har upptäckts. Följande logiska poster kommer att returneras:

— 1 post typ 1.

— 1 post typ 2.

Transaktionstypen ERR sammanfattas i tabell A.6.3 (bilaga 6).

Tabell 2: Tillåtna koder i transaktioner

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	—	—	—	—

Nyckel:

M = Obligatorisk
M* = Endast en av båda posttyperna får ingå
O = Frivillig
C = Beroende av tillgängliga uppgifter
– = Ej tillåten
1* = Beroende av legacy systems

3.1.5 Fält 1.005: Transaktionsdatum (*Date of Transaction – DAT*)

Detta fält anger vilken dag transaktionen initierades och måste följa ISO-standarden YYYYMMDD

där YYYY är året, MM är månaden och DD är dagen i månaden. Ledande nollor ska användas för ensiffriga tal. ”19931004” står till exempel för den 4 oktober 1993.

3.1.6 Fält 1.006: PRIORITET (*Priority – PRY*)

Detta frivilliga fält anger prioritet, på en nivå 1–9, för begäran. ”1” anger högsta prioritet, ”9” lägsta prioritet. Prioritet ”1” ska behandlas omedelbart.

3.1.7 Fält 1.007: Bestämmelseorgansidentifierare (Destination Agency Identifier – DAI)

Detta fält anger transaktionens bestämmelseorgan.

Det består av två uppgifter i följande format: CC/*organ*.

Den första uppgiften består av en landskod om två alfanumeriska tecken enligt ISO 3166. Den andra uppgiften, *organ*, identifierar organet genom en sträng fri text om maximalt 32 alfanumeriska tecken.

3.1.8 Fält 1.008: Ursprungsorgansidentifierare (*Originating Agency Identifier – ORI*)

Detta fält anger vilket organ som har skapat filen och har samma format som DAI (fält 1.007).

3.1.9 Fält 1.009: Transaktionskontrollnummer (*Transaction Control Number – TCN*)

Detta är ett kontrollnummer för hänvisningsändamål. Det bör skapas av datorn och ha följande format: YYSSSSSSSSA

där YY är år för transaktionen, SSSSSSSS är ett åttaställligt serienummer och A är ett kontrolltecken som har genererats med den procedur som anges i bilaga 2.

Om TCN inte är tillgängligt, ska fältet YYSSSSSSSS fyllas med nollor och det kontrolltecken som genererats enligt ovan.

3.1.10 Fält 1.010: Transaktionskontrollsvar (Transaction Control Response – TCR)

När en begäran har sänts med denna post som svar, innehåller detta frivilliga fält Transaction Control Number (TCN) för meddelandet med begäran. Det har därför samma format som TCN (fält 1.009).

3.1.11 Fält 1.011: (Native Scanning Resolution – NSR)

Detta fält anger den normala upplösningen vid skanning för det system som avsändaren av transaktionen använder. Upplösningen ska anges med två siffror följd av decimalpunkt och därefter ytterligare två siffror.

För alla transaktioner i enlighet med beslut 2008/615/RIF ska samplingsfrekvensen vara 500 pixel/tum eller 19,68 pixel/mm.

3.1.12 Fält 1.012: Nominell överföringsresolution (Nominal Transmitting Resolution – NTR)

Detta fält om fem positioner anger nominell överföringsupplösning för de bilder som överförs. Upplösningen ska uttryckas i pixel/mm i samma format som NSR (fält 1.011).

3.1.13 Fält 1.013: Domännamn (Domaine Name – DOM)

I detta obligatoriska fält anges domännamnet för den användardefinierade implementationen av logisk post typ 2. Det innehåller två uppgifter och ska uttryckas som "INT-I{US}4.22{GS}".

3.1.14 Fält 1.014: Greenwich Mean Time (GMT)

Detta obligatoriska fält ger möjlighet att uttrycka datum och tidpunkt i GMT-enheter (Greenwich Mean Time). Om det används innehåller GMT-fältet universellt datum i tillägg till det lokala datum som anges i fält 1.005 (DAT). Om GMT-fältet används elimineras inkonsekvenser med lokal tid när en transaktion och dess svar överförs mellan två platser skilda åt av flera tidszoner. GMT ger ett universellt datum och en 24-timmarstid som är oberoende av tidszoner. Fältet anges som "CCYYMMDDHHMMSSZ", en 15-positioners teckensträng som utgörs av datum konkatenerat med GMT och avslutas med "Z". Tecknen "CCYY" ska representera år för transaktionen, tecknen "MM" ska ange tiotals- och entalssiffran för månad, tecknen "DD" ska ange tiotals- och entalssiffran för dag i månaden, tecknen "HH" ska ange timme, "MM" ska ange minut och "SS" ska ange sekund. Den fullständiga tidsangivelsen får inte ange en tidpunkt i framtiden.

4. ***Logisk post typ 2: Beskrivande text***

Större delen av denna posts struktur definieras inte genom den ursprungliga ANSI/NIST-standarden. Posten innehåller information av särskilt intresse för de organ som sänder eller tar emot filen. För att säkerställa att de kommunicerande fingeravtryckssystemen är kompatibla kräver detta ICD att posten innehåller endast de fält som förtecknas nedan. I dokumentet anges vilka fält som är obligatoriska frivilliga, samtidigt som de enskilda fältens struktur fastställs.

4.1 *Fält i logisk post typ 2*

4.1.1 Fält 2.001: Logisk postlängd (*Logical Record Length – LEN*)

Detta obligatoriska fält anger längden av typ 2-posten i totalt antal byte, inklusive varje tecken i varje fält och informationsavgränsarna.

4.1.2 Fält 2.002: *Bilddesigneringstecken* (IDC)

Den IDC som anges i detta obligatoriska fält är en ASCII-representation av den IDC som definieras i fältet File Content i typ 1-posten.

4.1.3 Fält 2.003: Systeminformation (*System Information – SYS*)

Detta fält om fyra positioner är obligatoriskt och anger vilken version av INT-I som just denna typ 2-post följer.

I de första två positionerna anges versionsnumret, i de två följande revisionsnumret. Denna implementation grundar sig till exempel på INT-I version 2 revision 22, vilket ska uttryckas som "0422".

4.1.4 Fält 2.007: Ärendenummer (*Case Number – CNO*)

Detta är ett nummer som av det lokala fingeravtrycksorganet tilldelas en samling latenta avtryck som hittas på brottsplatsen. Följande format ska användas: CC/*nummer*

där "CC" är Interpols landskod med två alfanumeriska tecken och *nummer* följer de relevanta lokala riktlinjerna och kan bestå av upp till 32 alfanumeriska tecken.

Genom detta fält kan systemet identifiera latenta avtryck förknippade med ett visst brott.

4.1.5 Fält 2.008: Sekvensnummer (Sequence Number – SQN)

Detta specificerar varje sekvens av latenta avtryck inom ett fall. Det kan innehålla upp till fyra numeriska tecken. En sekvens är ett latent avtryck eller serier av latenta avtryck som förs samman i grupper för registrering och/eller sökning. Denna definition medför att även enskilda latenta avtryck måste tilldelas ett sekvensnummer.

Detta fält kan tillsammans med MID (fält 2.009) användas för att identifiera ett särskilt latent avtryck i sekvensen.

4.1.6 Fält 2.009: Latentavtrycksidentifierare (Latent Identifier – MID)

Detta fält specificerar det enskilda latenta avtrycket inom en sekvens. Värdet är en eller två bokstäver där ”A” tilldelas det första latenta avtrycket, ”B” tilldelas det andra och så vidare upp till gränsen ”ZZ”. Fältet används på samma sätt som sekvensnumret för det latenta avtrycket enligt beskrivningen av SQN (fält 2.008).

4.1.7 Fält 2.010: Brottsreferensnummer (Criminal Reference Number – CRN)

Detta är ett unikt referensnummer som ett nationellt organ tilldelar en person när denna för första gången döms för att ha begått ett brott. I ett visst land har en person aldrig mer än ett CRN, eller delar det med en annan person. Samma person kan emellertid ha Criminal Reference Numbers i flera länder, dessa kan då skiljas åt med hjälp av landskoden.

CRN-fältet ska ha följande format: CC/nummer

där ”CC” är landskod med två alfanumeriska tecken enligt ISO 3166 och *nummer* följer relevanta nationella riktlinjer från det utfärdande organet och kan bestå av upp till 32 alfanumeriska tecken.

I transaktioner i enlighet med beslut 2008/615/RIF kommer detta fält att användas för nationellt Criminal Reference Number från det organ som är kopplat till bilderna i poster av typ 4 eller typ 15.

4.1.8 Fält 2.012: (*Miscellaneous Identification Number – MN1*)

Detta fält innehåller det CRN (fält 2.010) som sänts med en CPS- eller PMS-transaktion, utan inledande landskod.

4.1.9 Fält 2.013: (*Miscellaneous Identification Number – MN2*)

Detta fält innehåller det CRO (fält 2.007) som sänts med en MPS- eller MMS-transaktion, utan inledande landskod.

4.1.10 Fält 2.014: (*Miscellaneous Identification Number – MN3*)

Detta fält innehåller det SQN (fält 2.008) som sänts med en MPS- eller MMS-transaktion.

4.1.11 Fält 2.015: (*Miscellaneous Identification Number – MN4*)

Detta fält innehåller det SQN (fält 2.009) som sänts med en MPS- eller MMS-transaktion.

4.1.12 Fält 2.063: Tilläggsinformation (*Additional Information – INF*)

Vid en SRE-transaktion efter en PMS-begäran informerar detta fält om vilket finger som gav anledning till den eventuella träffen. Fältet ska ha följande format:

NN där *NN* är den tvåställiga fingerpositionskod som definieras i tabell 5.

I alla övriga fall är detta fält frivilligt. Det består av upp till 32 alfanumeriska tecken och kan användas för att lämna ytterligare upplysningar om begäran.

4.1.13 Fält 2.064: (*Respondents List – RLS*)

Detta fält innehåller minst två delfält. Det första delfältet beskriver den typ av sökning som har gjorts med användning av den treställiga minneskod som specificerar transaktionstypen i TOT-fältet (fält 1.004). Det andra delfältet består av endast ett tecken. ”I” ska användas för att ange en TRÄFF, och ”N” ska användas för att ange att inga överensstämmelser har hittats (ICKE-TRÄFF). Det tredje delfältet innehåller sekvensidentifieraren för kandidatresultatet och totalt antal kandidater, avgränsat med snedstreck. Flera meddelanden kommer att returneras om det finns fler än en kandidat.

Vid en eventuell TRÄFF ska fjärde delfältet innehålla träffvärdet med upp till tio siffror. Om TRÄFFen har verifierats ska värdet för detta delfält definieras som ”999999”.

Exempel: ”CPS{RS}I{RS}001/001{RS}999999{GS}”

Om det AFIS till vilket transaktionen sänds inte tilldelar träffvärden, ska träffvärdet noll föras in på rätt plats.

4.1.14 Fält 2.074: Fält för status- och felmeddelanden (*Status/Error Message Field – ERM*)

Detta fält innehåller felmeddelanden vid transaktionsbearbetningen, vilka sänds tillbaka till den begärande parten som del av en feltransaktion.

Tabell 3: Felmeddelanden

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.

Felmeddelanden i intervallet 100–199:

Dessa felmeddelanden gäller kontrollen av ANSI/NIST-posterna och ska uttryckas som

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

där

— error_code är en kod som är entydigt kopplad till en viss orsak (se tabell 3),

— field_id är ANSI/NIST-fältnumret för det felaktiga fältet (t.ex. 1.001, 2.001, ...) i formatet <record_type>.<field_id>.<sub_field_id>,

— dynamic text är en mer utförlig situationsanpassad beskrivning av felet,

— LF är ett LF-tecken som avgränsar felen om fler än ett fel har påträffats,

— för typ 1-poster fastställs ICD till ”-1”.

Exempel:

201: IDC - 1 FIELD 1 009 FEL KONTROLLTECKEN {LF} 115: IDC 0 FIELD 2 003 OGILTIG SYSTEMINFORMATION

Detta fält är obligatoriskt för feltransaktioner.

4.1.15 Fält 2.320: Förväntat antal kandidater (*Expected Number of Candidates – ENC*)

Detta fält anger det maximala antal kandidater för kontroll som det begärande organet förväntar sig. Värdet ENC får inte överskrida de värden som definieras i tabell 11.

5. ***Logisk post typ 4: Högupplösningsbild i gråskala***

Det bör noteras att poster av typ 4 är binära poster snarare än ASCII-poster. Varje fält har där tilldelats en specifik position i posten, vilket medför att alla fält är obligatoriska.

Standarden medger att både bildstorlek och upplösning anges i posten. Logisk posttyp 4 måste innehålla fingeravtrycksuppgifter som överförs med en nominell pixeltäthet av 500–520 pixel/tum. Den täthet som föredras för nyutformningar är 500 pixel per tum, dvs. 19,68 pixel per mm. 500 pixel per tum är den täthet som specificeras i INT-I, med undantag för att liknande system får kommunicera med användning av en annan täthet inom intervallet 500–520 pixel per tum.

5.1 *Fält i logisk post typ 4*

5.1.1 Fält 4.001: Logisk postlängd (*Logical Record Length – LEN*)

Detta fält om fyra byte anger längden av typ 4-posten i totalt antal byte, inklusive varje byte i varje fält.

5.1.2 Fält 4.002: Bilddesigneringstecken (*Image Designation Character – IDC*)

Detta fält innehåller i binär form IDC-numret i filhuvudet.

5.1.3 Fält 4.003: Avtryckstyp (*Impression Type – IMP*)

Avtryckstyp är ett fält om en byte i sjätte positionen i posten.

Tabell 4: Fingeravtryckstyp

	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

	Description
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4 Fält 4.004: Fingerposition (Finger Position – FGP)

Detta fasta fält med 6 byte upptar positionerna 7–12 i en post av typ 4. Det innehåller möjliga fingerställningar med början i den byte som befinner sig längst till vänster (byte 7 i posten). Känd eller mest trolig fingerposition har tagits från tabell 5. Upp till fem ytterligare fingrar kan registreras genom att man lägger in alternerande fingerpositioner i återstående fem byte i samma format. Om färre än fem fingerpositionsreferenser används fylls oanvända byte med binära 255. För att registrera alla fingerpositioner används 0 för okänd.

Tabell 5: Fingerposition och maximal storlek

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

För latenta fingeravtryck på brottsplatsen bör endast koderna 0-10 användas.

5.1.5 Fält 4.005: Bildskanningsupplösning (*Image Scanning Resolution – ISR*)

Detta fält om en byte upptar position 13 i typ 4-posten. Om det innehåller ”0” har bilden skannats med en föredragen upplösning på 19,68 pixel/mm (500 pixel per tum). Om det innehåller ”1” har bilden skannats med en alternativ upplösning enligt typ 1-posten.

5.1.6 Fält 4.006: Horisontell linjelängd (*Horizontal Line Length – HLL*)

I detta fält som upptar positionerna 14-15 i typ 4-posten anges antalet pixel i varje skanningslinje. Den första positionen är mest signifikant.

5.1.7 Fält 4.007: Vertikal linjelängd (*Vertical Line Length – VLL*)

I detta fält i positionerna 16–17 anges antalet skanningslinjer i bilden. Den första positionen är mest signifikant.

5.1.8 Fält 4.008: Algoritm för komprimering av gråskalan (*Gray-scale Compression Algorithm – GCA*)

I detta fält om en byte anges vilken algoritm för komprimering av gråskalan som har använts för att koda bilddata. En binär kod 1 anger att WSQ-komprimering (bilaga 7 har använts för denna implementation.

5.1.9 Fält 4.009: Bilden (*The Image*)

Detta fält innehåller en teckensträng som representerar bilden. Fältets struktur kommer uppenbarligen att vara beroende av vilken komprimeringsalgoritm som används.

6. ***Logisk post typ 9: Minutiaepost***

Typ 9-poster ska innehålla ASCII-text som beskriver minutiae och dithörande uppgifter som har registrerats från ett latent avtryck. För en sökning efter latenta avtryck finns ingen övre gräns för antalet typ 9-poster i filen, som var och en ska svara mot en annan vy eller latent avtryck.

6.1 *Extraktion av minutiae*

6.1.1 Identifiering av minutiaetypen

I denna standard definieras tre identifikationsnummer som används för att beskriva minutiaetypen. Dessa specifikationer förtecknas i tabell 6. Åsavslutningar ska betecknas typ 1. Förgreningar ska betecknas typ 2. Om en minutiae inte klart kan kategoriseras en av de ovan nämnda typerna ska den betecknas som ”annan”, typ 0.

Tabell 6: Minutiaetyper

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2 Typ och placering av minutiae

För att mallarna ska uppfylla kraven i avsnitt 5 i standarden ANSI INCITS 378-2004, ska följande metod, som förstärker den nu gällande standarden INCITS 378-20204, användas för att bestämma placering (läge och vinkelriktning) för enskilda minutiae.

Positionen eller läget för en minutia som representerar avslutningen på en ås ska vara gaffelpunkten i dalområdets mittskelett omedelbart framför åsavslutningen. Om de tre benen i dalområdet tunnas ner till en skelettbild som är en enda pixel bred, är det skärningspunkten som är minutians läge. På samma sätt blir minutialäget för en förgrening förgreningspunkten för linjens mittskelett. Om de tre benen i åsen tunnas ner till en skelettbild som är en enda pixel bred är det skärningspunkten för de tre benen som är minutians läge.

När alla linjeslut har omvandlats till förgreningar, framställs alla minutiae i fingeravtrycksbilden som förgreningar. X- och Y-pixelkoordinaterna för skärningen av de tre benen i varje minutia kan direktformateras. Bestämning av minutiariktningen kan extraheras from varje skelettförgrening. De tre benen i varje skelettförgrening måste undersökas, och avslutningspunkten för varje ben bestämmas. Figur 6.1.2 illustrerar de tre metoder som används för att bestämma avslutningen på ett ben som grundar sig på en skanningsupplösning på 500 ppi.

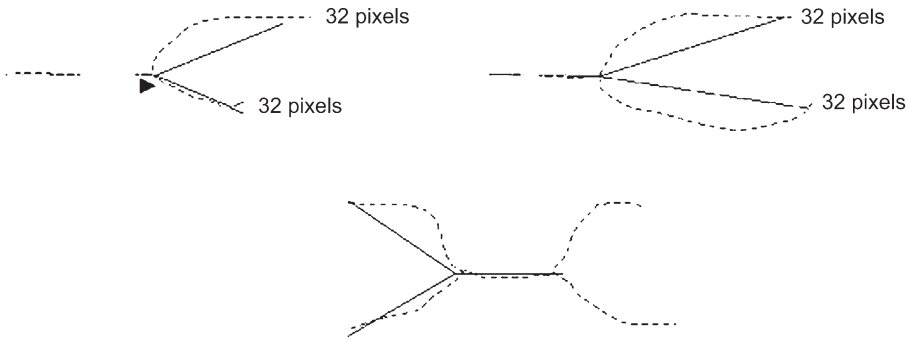
Avslutningen fastställs i enlighet med det som först inträffar. Pixelantalet grundar sig på en skanningsupplösning på 500 ppi. Olika skanningsupplösningar innebär olika pixelantal.

— Ett avstånd på .064 tum (den 32:a pixeln).

— Avslutningen på skelettbenet som inträffar mellan ett avstånd på .02 tum och .064 tum (den 10:e till den 32:a pixeln. Kortare ben används ej.

— En andra förgrening uppträder inom ett avstånd på .064 tum (före den 32:a pixeln).

Figur 6.1.2



Minutiavinkeln bestäms genom att man drar tre virtuella strålar som utgår från gaffelpunkten och fortsätter till avslutningen av varje ben. Den minsta av de tre vinklar som bildas av strålarna skärs av på mitten för att ange minutians riktning.

6.1.3 Koordinatsystem

Det koordinatsystem som används för att beskriva minutiae i ett fingeravtryck ska vara ett rätvinkligt koordinatsystem med två axlar. Läge för minutiae ska anges med deras x- och y-koordinater. Koordinatsystemet ska ha origo i det övre vänstra hörnet av den ursprungliga bilden, med x-axeln pekande åt höger och y-axeln pekande nedåt. Både x-koordinaten och y-koordinaten för en minutia ska anges i pixlar från origo. Det bör noteras att läget för origo och måttenheten inte stämmer med definitionen av typ 9-poster i ANSI/NIST-ITL 1-2000.

6.1.4 Minutiaeriktning

Vinklar ska uttryckas i vanlig matematisk form, med nollgrader åt höger och vinkelvärden som ökar moturs. Registrerade vinklar pekar i riktningen tillbaka längs åsen på en avslutning av åsen och mot dalens centrum på en förgrening. Enligt denna konvention avviker vinklarna 180 grader från vad som anges i definitionen poster av typ 9 i ANSI/NIST-ITL 1-2000.

6.2 *Fält i poster av typ 9, INCITS-378-format*

Samtliga fält i typ 9-poster ska registreras som ASCII-text. I denna posttyp med taggade fält tillåts inga binära fält.

6.2.1 Fält 9.001: Logisk postlängd (*Logical record length – LEN*)

I detta obligatoriska fält anges längden av den logiska posten som det sammanlagda antalet byte i varje fält i posten.

6.2.2 Fält 9.002: (Image Designation Character – IDC)

Detta obligatoriska fält om två positioner ska användas för att identifiera och ange läge för minutiaeuppgifterna. IDC i detta fält ska stämma överens med IDC i filinnehållsfältet i typ 1-posten.

6.2.3 Fält 9.003: (Impression Type – IMP)

Detta obligatoriska fält om en byte ska beskriva på vilket sätt informationen i fingeravtrycksbilden har erhållits. ASCII-värdet för rätt kod för avtryckstypen ur tabell 4 ska registreras i detta fält.

6.2.4 Fält 9.004: Minutiaeformat (*Minutiæ format – FMT*)

Detta fält ska innehålla ”U” för att ange att minutiae är formaterade enligt M1-378. Även om informationen kan ha kodats enligt M1-378-standarden, måste samtliga fält i typ 9-posten förbli fält med ASCII-text.

6.2.5 Fält 9.126: CBEFF-information (*CBEFF-information*)

Detta fält ska innehålla tre uppgifter. Den första uppgiften ska ha värdet ”27” (0x1B). Detta är en identifikation av ägaren av CBEFF-formatet som har tilldelats INCITS:s tekniska kommitté M1 av International Biometric Industry Association (IBIA). <US>-avgränsaren ska avgränsa denna uppgift från CBEFF-formattypen som har tilldelats värdet ”513” (0x0201), vilket anger att denna post endast innehåller uppgifter om läge och vinkelriktning utan att

ange någon information ur Extended Data Block. <US>-avgränsaren ska avgränsa denna uppgift från CBEFF-produktidentifieraren (PID) som identifierar ”ägaren” av kodningsutrustningen. Det är säljaren som fastställer detta värde. Det kan erhållas från IBIA:s webbplats (www.ibia.org) om det har publicerats på webben.

6.2.6 Fält 9.127: Identifikation av upptagningsutrustning (*Capture equipment identification*)

Detta fält ska innehålla två uppgifter skilda åt med <US>-avgränsaren. Den första uppgiften ska innehålla ”APPF”, om den utrustning som användes för att ursprungligen ta upp bilden var certifierad att överensstämma med bilaga F (Bildkvalitetsspecifikation för IAFIS, 29 januari 1999) till FBI:s specifikation för överföring av fingeravtryck i elektronisk form CJIS-RS-0010. Om utrustningen inte överensstämmer med denna specifikation, ska fältet innehålla teckensträngen ”NONE”. Den andra uppgiften ska innehålla upptagningsutrustningens identifikationsbegrepp (Capture Equipment ID), ett produktnummer för upptagningsutrustningen som tilldelats av säljaren. Värdet ”0” anger att upptagningsutrustningens identifikationsbegrepp inte har rapporterats.

6.2.7 Fält 9.128: Horisontell linjelängd (*Horizontal Line Length – HLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet pixel i en enstaka horisontell linje i den överförda bilden. Storleken i horisontell led är begränsad till 65 534 pixel.

6.2.8 Fält 9.129: Vertikal linjelängd (*Vertical Line Length – VLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet horisontella linjer i den överförda bilden. Storleken i vertikal led är begränsad till 65 534 pixel.

6.2.9 Fält 9.130: Skalenheter (*Scale units – SLC*)

Detta obligatoriska ASCII-fält ska ange enhet för samplingsfrekvensen (pixeltätheten). ”1” i detta fält anger pixel per tum, ”2” anger pixel per centimeter. ”0” i detta fält betyder att ingen enhet har angivits. I detta fall ger kvoten HPS/VPS pixelsidförhållandet (pixel aspect ratio).

6.2.10 Fält 9.131: Horisontell pixelskala (*Horizontal pixel scale – HPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i horisontell led, förutsatt att SLC innehåller ”1” eller ”2”. I annat fall anger det den horisontella komponenten av pixelsidförhållandet (pixel aspect ratio).

6.2.11 Fält 9.132: Vertikal pixelskala (*Vertical pixel scale – VPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i vertikal led, förutsatt att SLC innehåller ”1” eller ”2”. I annat fall anger det den vertikala komponenten av pixelsidförhållandet (pixel aspect ratio).

6.2.12 Fält 9.133: Fingervy (*Finger view*)

Detta obligatoriska fält innehåller vynumret för det finger postens uppgifter avser. Vynumren börjar på ”0” och ökar till ”15” med steglängden ett.

6.2.13 Fält 9.134: Fingerposition (*Finger Position – FGP*)

Detta fält ska innehålla koden för den fingerposition som lämnade informationen i denna typ 9-post. En kod mellan 1 och 10 från tabell 5, eller rätt handflatekod från tabell 10, ska användas för att ange finger- eller handflateposition.

6.2.14 Fält 9.135: Fingerkvalitet (*Finger quality*)

Detta fält ska ange den sammanlagda kvaliteten för uppgifterna om fingerminutiae med ett värde mellan 0 och 100. Detta tal sammanfattar fingerpostens kvalitet och avspeglar originalbildens kvalitet, kvaliteten vid extrahering av minutiae och andra operationer som kan påverka minutiaeposten.

6.2.15 Fält 1.136: Minutiaeantal (*Number of minutiae*)

I detta obligatoriska fält ska antalet minutiae som registrerats i denna logiska post anges.

6.2.16 Fält 9.137: Uppgifter om fingerminutiae (*Finger minutiæ data*)

Detta fält ska innehålla sex uppgifter åtskilda med <US>-avgränsaren. Det består av flera delfält där vart och ett innehåller detaljerna för enskilda minutiae. Det totala antalet minutiaedelfält måste stämma överens med antalet i fält 136. Den första uppgiften är minutiaeindexnummer, som ska initialiseras till ”1” och ökas med ”1” för varje tillkommande minutia i fingeravtrycket. Den andra och den tredje uppgiften är x-koordinaten och y-koordinaterna för minutiae i pixelenheter. Den fjärde uppgiften är minutiaevinkeln angiven i enheter om två grader. Detta värde ska vara icke-negativt mellan 0 och 179. Den femte uppgiften är minitiaetypen. Ett värde av ”0” används för att representera minutiae av typen ”ANNAN”, ett värde av ”1” för en åsavslutning och ett värde av ”2” för en åsförgrening. Den sjätte uppgiften anger kvaliteten för varje minutiae. Värdet ska ligga mellan minst 1 och mest 100. Ett ”0”-värde anger att kvalitetsvärde saknas. Varje delfält ska skiljas från nästa delfält med <RS>-avgränsaren.

6.2.17 Fält 9.138: Uppgifter om åsantal (*Ridge count information*)

Fältet består av en serie delfält där vart och ett innehåller tre uppgifter. Den första uppgiften i det första delfältet ska ange metoden för extrahering av antal åsar. ”0” anger att metoden för att extrahera antalet åsar är okänd, liksom ordningen i posten. ”1” anger att för varje centrumminutia har uppgifter om åsantal tagits fram till närmaste angränsande minutia i fyra kvadranter, och åsantal för varje centrumminutia har förtecknats tillsammans. ”2” anger att för varje centrumminutia har uppgifter om åsantal tagits fram till närmaste grannminutia i fyra kvadranter, och åsantal för varje centrumminutia har förtecknats tillsammans. De återstående två uppgifterna i det första delfältet ska båda innehålla ”0”. Uppgifterna ska åtskiljas av <US>-avgränsaren. Följande delfält får centrumminutians indexnummer som första uppgift, indexnummer för angränsande minutiae som andra uppgift och antalet åsövergångar som tredje uppgift. Uppgifterna ska åtskiljas av <US>-avgränsaren.

6.2.18 Fält 9.139: Uppgifter om centrumpunkter (*Core information*)

Detta fält består av ett delfält för varje centrumpunkt i originalbilden. Varje delfält innehåller tre uppgifter. De första två uppgifterna innehåller x- och y-koordinatpositionerna i pixelenheter. Den tredje uppgiften innehåller centrumpunktens vinkel angiven i enheter om 2 grader. Detta värde ska vara icke-negativt mellan 0 och 179. Multipla centrumpunkter ska åtskiljas av <RS>-avgränsaren.

6.2.19 Fält 9.140: Deltauppgifter (*Delta information*)

Detta fält består av ett delfält för varje deltapunkt i originalbilden. Varje delfält innehåller tre uppgifter. De första två uppgifterna innehåller x- och y-koordinatpositionerna i pixelenheter. Den tredje uppgiften innehåller deltapunktens vinkel angiven i enheter av 2 grader. Detta värde ska vara icke-negativt mellan 0 och 179. Multipla centrumpunkter ska åtskiljas av <RS>-avgränsaren.

7. ***Post typ 13: Bilder av latenta avtryck med varierande upplösning***

Logisk post av typ 13 med taggade fält ska innehålla data från bilder av latenta avtryck. Dessa bilder är avsedda att överföras till organ som automatiskt extraherar eller använder mänsklig intervention och behandling för att extrahera den önskade detaljinformationen från bilderna.

Uppgifter om skanningsupplösning, bildstorlek och andra parametrar som krävs för att behandla bilden registreras som taggade fält inom posten.

Tabell 7: Post typ 13: Bilder av latenta avtryck med varierande upplösning

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 ALG-ORITHM	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	—

Nyckel för teckentyp: N = numerisk, A = alfabetisk, AN = alfanumerisk, B = binär

7.1 *Fält i logisk post typ 4*

Följande stycken beskriver uppgifterna i vart och ett av fälten för logisk post typ 13.

Inom en logisk post typ 13 ska registreringar läggas in i numrerade fält. De första två fälten i posten måste vara i rätt ordning, och fältet med bilduppgifterna ska vara det sista fysiska fältet i posten. För varje fält i typ 13-posten förtecknas i tabell 7 koden ”Beroende på tillgång på uppgifter” (”condition code”) som obligatorisk ”M” eller frivillig/valfri ”O”, fältnummer, fältbenämning, teckentyp, fältstorlek och förekomstgränser. Maximal storlek för fältet, uttryckt i antal byte och grundad på ett treställigt fältnummer, anges i sista kolumnen. När fler siffror används för fältnumret ökar också maximalt antal byte. De två registreringarna i fältstorlek per förekomst (”field size per occurrence”) inkluderar alla teckenavgränsare i fältet. Maximalt antal byte (”Maximum byte count”) inkluderar fältnummer, uppgifter och alla teckenavgränsare inklusive <GS>-avgränsaren.

7.1.1 Fält 13.001: Logisk postlängd (*Logical record length – LEN*)

I detta obligatoriska fält anges det totala antalet byte i hela logisk post typ 1. I fält 13.001 anges postens längd inklusive alla tecken i alla fält i posten samt uppgiftsavgränsare.

7.1.2 Fält 13.002: Bilddesigneringstecken (*Image Designation Character – IDC*)

Detta obligatoriska ASCII-fält ska användas för att identifiera bilduppgifterna om latent avtryck i posten. Detta IDC ska matcha IDC i fältet för filinnehåll (CNT) i typ 1-posten.

7.1.3 Fält 13.003: Avtryckstyp (*Impression Type – IMP*)

Detta obligatoriska fält om en eller två byte ska beskriva på vilket sätt bildinformationen om det latenta avtrycket har erhållits. Korrekt latentkod från tabell 4 (finger) eller tabell 9 (handflata) ska föras in i detta fält.

7.1.4 Fält 13.004: Källorgan (*Source agency/ORI – SRC*)

Detta obligatoriska ASCII-fält ska innehålla identifikation av den myndighet eller organisation som ursprungligen tog upp ansiktsbilden i posten. Normalt sett är det ursprungsorgansidentifieraren för det organ som tog upp bilden som ska stå i detta fält. Det består av två uppgifter i följande format: CC/*organ*.

Den första uppgiften består av Interpols landskod om två alfanumeriska tecken. Den andra uppgiften, *organ*, identifierar organet genom en sträng fri text om maximalt 32 alfanumeriska tecken.

7.1.5 Fält 13.005: Upptagningsdatum för latent avtryck (*Latent capture date – LCD*)

Detta obligatoriska ASCII-fält ska innehålla datum för upptagningen av den latenta bilden i posten. Datum skrivs som åtta siffror i formatet CCYYMMDD. CCYY-tecknen står för året för upptagningen av bilden. MM-tecknen är månadens tiotals- och enhetsvärden och DD-tecknen tiotals- och enhetsvärden för dagen i månaden. Till exempel står 20000229 för den 29 februari 2000. Fullständigt datum måste vara ett riktigt datum.

7.1.6 Fält 13.065: Horisontell linjelängd (*Horizontal Line Length – HLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet pixel i en enstaka horisontell linje i den överförda bilden.

7.1.7 Fält 13.007: Vertikal linjelängd (*Vertical Line Length – VLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet horisontella linjer i den överförda bilden.

7.1.8 Fält 13.008: Skalenheter (*Scale units – SLC*)

Detta obligatoriska ASCII-fält ska ange enhet för samplingsfrekvensen (pixeltätheten). ”1” i detta fält anger pixel per tum, ”2” anger pixel per centimeter. ”0” i detta fält betyder att ingen enhet har angivits. I detta fall ger kvoten HPS/VPS pixelsidförhållandet (pixel aspect ratio).

7.1.9 Fält 13.009: Horisontell pixelskala (*Horizontal pixel scale – HPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i horisontell led, förutsatt att SLC innehåller ”1” eller ”2”. I annat fall anger det den horisontella komponenten av pixelsidförhållandet (pixel aspect ratio).

7.1.10 Fält 13.010: Vertikal pixelskala (*Vertical pixel scale – VPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i vertikal led, förutsatt att SLC innehåller ”1” eller ”2”. I annat fall anger det den vertikala komponenten av pixelsidförhållandet (pixel aspect ratio).

7.1.11 Fält 13.011: Komprimeringsalgoritm (*Compression algoritm – CGA*)

Detta obligatoriska ASCII-fält ska ange den algoritm som används för att komprimera gråskalebilder. Komprimeringskoderna anges i bilaga 7.

7.1.12 Fält 13.012: Bitar per pixel (*Bits per pixel – BPX*)

Detta obligatoriska ASCII-fält ska innehålla antalet bitar som används för en pixel. I detta fält står ”8” för normala gråskalevärden från ”0” till ”255”. Alla värden i detta fält som är större än ”8” står för gråskalepixel med högre precision.

7.1.13 Fält 13.013: Fingerposition/handflateposition (*Finger/Palm Position – FGP*)

Detta obligatoriska taggade fält ska innehålla en eller flera av de möjliga finger-/handflatepositioner som kan matcha den latenta bilden. Det decimalkodsnummer som motsvarar den kända eller mest troliga fingerpositionen ska tas från tabell 5 eller den mest troliga handflatepositionen från tabell 10 och föras in som ett ASCII-delfält med ett eller två tecken. Ytterligare finger- och/eller handflatepositioner kan registreras genom att man lägger in alternerande positionskoder som delfält åtskilda av RS-avgränsaren. Koden ”0” för ”Okänt finger” ska användas för att registrera varje fingerposition från ett till tio. Koden ”20” för ”Okänd handflata” ska användas för att registrera varje handflateposition i förteckningen.

7.1.14 Fält 13.014-019: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

7.1.15 Fält 13.020: Kommentar (*Comment COM*)

Detta frivilliga fält kan användas för kommentarer eller annan information i ASCII-text med uppgifter om latent bild.

7.1.16 Fält 13.021-199: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

7.1.17 Fält 13.200-998: Användardefinierade fält (*User-defined fields – UDF*)

Dessa fält är användardefinierade fält och kommer att användas för framtida behov. Deras storlek och innehåll ska definieras av användaren i enlighet med det mottagande organet. Om de förekommer ska de innehålla information i ASCII-text.

7.1.18 Fält 13.999: Bilduppgifter (*Image data – DAT*)

Detta fält ska innehålla alla uppgifter från en upptagen latent bild. Det ska alltid få fältnummer 999 och måste vara det sista fysiska fältet i posten. Till exempel följs ”13.999” av bilduppgifter i binärt format.

Varje pixel av okomprimerade gråskaleuppgifter ska normalt kvantifieras till åtta bitar (256 grå nivåer) i en enda byte. Om värdet i BPX-fältet 13.102 är större än eller mindre än ”8” får man ett annat antal byte som krävs för att innehålla en pixel. Om komprimering används ska pixeluppgifterna komprimeras i enlighet med den komprimeringsteknik som anges i GCA-fältet.

7.2 *Avslutning post typ 13: Latenta bilder med varierande upplösning*

Omedelbart efter sista byte uppgifter från fält 13.199 ska för konsekvensens skull en <FS>-avgränsare användas för att avgränsa den från nästa logiska post. Denna avgränsare måste inkluderas i typ 13-postens längdfält.

8. ***Post typ 15: Bilder av handavtryck med varierande upplösning***

Det taggade fältet i logisk post typ 15 ska innehålla och användas för att utbyta uppgifter om handflateavtryck tillsammans med fasta och användardefinierade textinformationsfält avseende den digitaliserade bilden. Uppgifter om skanningsupplösning, bildstorlek och andra parametrar eller kommentarer som krävs för att behandla bilden registreras som taggade fält inom posten. Handflateavtrycksbilder som översänds till andra organ kommer att behandlas av de mottagande organen för att extrahera den önskade detaljinformation som krävs för matchning.

Bilduppgifterna fås direkt från en person med hjälp av en livescan-utrustning eller från en handflateavtrycksblankett eller annat medium som innehåller personens handflateavtryck.

Alla metoder som används för att få fram bilder av handflateavtrycket ska också medge upptagning av en uppsättning bilder för varje hand. Denna uppsättning ska inkludera handflatans yttre kant som en enda skannad bild och hela området för hela handen från handleden till fingertopparna som en eller två skannade bilder. Om två bilder används för att visa hela handflatan, ska den nedre bilden visa området från handleden till övre delen av området mellan fingrarna (tredje fingerleden) inklusive områdena kring handflatans tumvalk och lillfingervalk. Den övre bilden ska visa området från nedre delen av det interdigitala området till de översta fingertopparna. Detta ger tillräcklig överlappning mellan de två bilderna som båda visar handflateområdet mellan fingrarna. Genom att matcha åsstrukturen och detaljerna i detta gemensamma område kan en undersökare med tillförlitlighet konstatera att båda bilderna kom från samma handflata.

Eftersom en handavtryckstransaktion kan användas för olika ändamål, kan det innehålla ett eller flera unika bildområden registrerade från handflatan eller handen. En fullständig registrering av ett handflateavtryck från en individ inkluderar normalt handflatans yttre kant och fullständig/a bild/er av varje handflata. Eftersom en logisk bildpost med taggade fält kan innehålla endast ett binärt fält, kommer det att krävas en enda typ 15-post för varje handflatekant och en eller två typ 15-poster för varje fullständig handflata. Därför behövs det fyra till sex typ 15-poster för att visa personens handflateavtryck i en normal transaktion med handflateavtryck.

8.1 *Fält i logisk post typ 15*

Följande stycken beskriver uppgifterna i vart och ett av fälten för logisk post typ 15.

Inom en logisk post typ 15 ska registreringar läggas in i numrerade fält. De första två fälten i posten måste vara i rätt ordning, och fältet med bilduppgifterna ska vara det sista fysiska fältet i posten. För varje fält i typ 15-posten förtecknas i tabell 8 korskoden ”Beroende av tillgång på uppgifter” (”condition code”) som obligatorisk ”M” eller frivillig/valfri ”O”, fältnummer, fältbenämning, teckentyp, fältstorlek och förekomstgränser. Maximal storlek för fältet, uttryckt i antal byte och grundad på ett treställigt fältnummer, anges i sista kolumnen. När fler siffror används för fältnumret ökar också maximalt antal byte. De två registreringarna i fältstorlek per förekomst (”field size per occurrence”) inkluderar alla teckenavgränsare i fältet. Maximalt antal byte (”Maximum byte count”) inkluderar fältnummer, uppgifter och alla teckenavgränsare inklusive GS-avgränsaren.

8.1.1 Fält 15.001: Logisk postlängd (*Logical record length – LEN*)

I detta obligatoriska ASCII-fält anges det totala antalet byte i hela den logiska posten av typ 15. I fält 15.001 ska anges postens längd inklusive alla tecken i alla fält i posten samt uppgiftsavgränsare.

8.1.2 Fält 15.002: Bildbenämningstecken (*Image Designation Character – IDC*)

Detta obligatoriska ASCII-fält ska användas för att identifiera uppgifterna om handflateavtrycksbilden i posten. Detta IDC ska matcha IDC i fältet för filinnehåll (CNT) i typ 1-posten.

8.1.3 Fält 15.003: Avtryckstyp (*Impression Type – IMP*)

Detta obligatoriska ASCII-fält om en byte ska ange på vilket sätt informationen i handavtrycksbilden har erhållits. Korrekt kod från tabell 9 ska föras in i detta fält.

8.1.4 Fält 15.004: Källorgan (*Source agency/ORI – SRC*)

Detta obligatoriska ASCII-fält ska innehålla identifikation av den myndighet eller organisation som ursprungligen tog upp ansiktsbilden i posten. Normalt sett är det ursprungsorgansidentifieraren för det organ som tog upp bilden som ska stå i detta fält. Det består av två uppgifter i följande format: CC/*organ*.

Den första uppgiften består av Interpols landskod om två alfanumeriska tecken. Den andra uppgiften, *organ*, identifierar organet genom en sträng fri text om maximalt 32 alfanumeriska tecken.

8.1.5 Fält 15.005: Upptagningsdatum för handflateavtrycket (*Palmprint capture date – PCD*)

Detta obligatoriska ASCII-fält ska ange datum för upptagningen av handflateavtrycket. Datum skrivs som åtta siffror i formatet CCYYMMDD. CCYY-tecknen står för året för upptagningen av bilden. MM-tecknen ska ange tiotals- och entalssiffran för månaden och DD-tecknen tiotals- och entalssiffran för dagen i månaden. Till exempel står 20000229 för den 29 februari 2000. Fullständigt datum måste vara ett verkligt datum.

8.1.6 Fält 15.006: Horisontell linjelängd (*Horizontal Line Length – HLL*)

Detta obligatoriska ASCII-fält ska innehålla antalet pixlar i en enstaka horisontell linje i den överförda bilden.

8.1.7 Fält 15.007: Vertikal linjelängd (*Vertical Line Length – VLL*)

Detta obligatoriska ASCII-fält ska ange antalet horisontella linjer i den överförda bilden.

8.1.8 Fält 15.008: Skalenheter (*Scale units – SLC*)

Detta obligatoriska ASCII-fält ska ange enhet för samplingsfrekvensen (pixeltätheten). ”1” i detta fält anger pixel per tum, ”2” anger pixel per centimeter. ”0” i detta fält betyder att ingen enhet har angivits. I detta fall ger kvoten HPS/VPS pixelsidförhållandet (pixel aspect ratio).

8.1.9 Fält 15.009: Horisontell pixelskala (*Horizontal pixel scale – HPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i horisontell led, förutsatt att SLC innehåller ”1” eller ”2”. I annat fall anger det den horisontella komponenten av pixelsidförhållandet (pixel aspect ratio).

8.1.10 Fält 15.010: Vertikal pixelskala (*Vertical pixel scale – VPS*)

Detta obligatoriska ASCII-fält ska ange heltalsvärdet av pixeltätheten i vertikal led, förutsatt att SLC innehåller ”1” eller ”2”. I annat fall anger det den vertikala komponenten av pixelsidförhållandet (pixel aspect ratio).

Tabell 8: Post typ 15: Bilder av handflateavtryck med varierande upplösning

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	—

Tabell 9: Handflateavtryckstyp

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 Fält 15.011: Komprimeringsalgoritm (*Compression algoritm – CGA*)

Detta obligatoriska ASCII-fält ska ange den algoritm som används för att komprimera gråskalebilder. ”NONE” i detta fält anger att uppgifterna i denna post inte har komprimerats. För de uppgifter som ska komprimeras ska detta fält innehålla den metod som valts för komprimering av fingeravtrycksbilder av 10 fingrar. Giltiga komprimeringskoder definieras i bilaga 7.

8.1.12 Fält 15.012: Bitar per pixel (*Bits per pixel – BPX*)

Detta obligatoriska ASCII-fält ska innehålla antalet bitar som används för en pixel. I detta fält ska ”8” stå för normala gråskalevärden från ”0” till ”255”. Alla värden i detta fält som är större än eller mindre än ”8” står för en gråskalepixel med högre respektive lägre precision.

Tabell 10: Handflatekoder, områden och storlekar

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 Fält 15.013: Handavtrycksposition (Palmprint position – PLP)

Detta obligatoriska taggade fält ska innehålla den handavtrycksposition som matchar bilden av handflateavtrycket. Det decimalkodsnummer som motsvarar den kända eller mest troliga handavtryckspositionen ska tas från tabell 10 och föras in som ett ASCII-delfält med ett eller två tecken. Tabell 10 listar också maximala bildområden och dimensioner för var och en av de möjliga positionerna för handavtrycken.

8.1.14 Fält 15.014-019: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

8.1.15 Fält 15.020: Kommentar (*Comment – COM*)

Detta frivilliga fält kan användas för kommentarer eller annan information i ASCII-text med uppgifter om handavtrycksbild.

8.1.16 Fält 15.021-199: Reserverad för framtida definition (*Reserved for future definition – RSV*)

Dessa fält har reserverats för att ingå i framtida revisioner av denna standard. Inget av dessa fält får användas i denna revision. Om något av fälten förekommer ska de lämnas utan avseende.

8.1.17 Fält 15.200-998: Användardefinierade fält (*User-defined fields – UDF*)

Dessa fält är användardefinierade fält och kommer att användas för framtida behov. Deras storlek och innehåll ska definieras av användaren i enlighet med det mottagande organet. Om de förekommer ska de innehålla information i ASCII-text.

8.1.18 Fält 15.999: Bilduppgifter (*Image data – DAT*)

Detta fält ska innehålla alla uppgifter om en upptagen handavtrycksbild. Det ska alltid tilldelas fältnummer 999 och måste vara det sista fysiska fältet i posten. Till exempel ”15.999” följs av bilduppgifter i binärt format. Varje pixel av okomprimerade gråskaleuppgifter ska normalt kvantifieras till åtta bitar (256 grå nivåer) i en enda byte. Om värdet i BPX-fältet 15.012 är större än eller mindre än ”8” får man ett annat antal byte som krävs för att innehålla en pixel. Om komprimering används ska pixeluppgifterna komprimeras i enlighet med den komprimeringsteknik som anges i CGA-fältet.

8.2 *Avslutning post typ 15: Handavtrycksbilder med varierande upplösning*

Omedelbart efter sista byte av uppgifter från fält 15.999 ska för konsekvensens skull en <FS>-avgränsare användas för att avgränsa den från nästa logiska post. Denna avgränsare måste inkluderas i typ 15-postens längdfält.

8.3 *Ytterligare handavtrycksbilder av post typ 15 med varierande upplösning*

Ytterligare typ 15-poster kan inkluderas i filen. För varje ytterligare handavtrycksbild krävs en fullständig logisk post typ 15 tillsammans med <FS>-avgränsaren.

Tabell 11: Högsta för verifiering godtagna antal kandidater per sändning

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

Sökningstyper:

TP/TP: tiofingersavtryck mot tiofingersavtryck

LP/TP: latent fingeravtryck mot tiofingersavtryck

LP/PP: latent handflateavtryck mot handflateavtryck

TP/UL: tiofingersavtryck mot olöst latent fingeravtryck

LT/UL: latent fingeravtryck mot olöst latent fingeravtryck

PP/ULP: handflateavtryck mot olöst latent handflateavtryck

LP/ULP: latent handflateavtryck mot olöst latent handflateavtryck

9. ***Bilagor till kapitel 2 (utbyte av finger- och handavtrycksuppgifter)***

9.1 *Bilaga 1 ASCII-koder för avgränsare*

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

([1]) Detta är positionen enligt definitionen i ASCII-standarden.

9.2 *Bilaga 2 Beräkning av alfanumeriskt kontrolltecken*

För TCN och TCR (Fält 1.09 och 1.10)

Det tal som motsvarar kontrolltecknet genereras enligt följande formel:

(YY * 10^8 + SSSSSSSS) Modulo 23

där YY and SSSSSSSS är de numeriska värdena av de sista två siffrorna för år respektive serienummer.

Kontrolltecknet genereras sedan ur tabellen nedan.

För CRO (Fält 2.010)

Det tal som motsvarar kontrolltecknet genereras enligt följande formel:

(YY * 10^6 + NNNNNN) Modulo 23

där YY and SSSSSSSS är de numeriska värdena av de sista två siffrorna för år respektive serienummer.

Kontrolltecknet genereras sedan ur tabellen nedan.

Kontrollteckentabell

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 *Bilaga 3 Teckenkoder*

7-bitars ANSI-kod för informationsutbyte

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 *Bilaga 4 Sammanfattning av transaktioner*

Post typ 1 (obligatorisk)

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

Under villkorskolumnen:

O = frivilligt, M = obligatoriskt, C = beroende på om transaktionen är ett svar till ursprungsorganet

Post typ 2 (obligatorisk)

Identifier	Field Number	Field Name	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

Under kolumnen ”Condition”:

O = frivilligt, M = obligatoriskt, C = beroende av tillgängliga uppgifter

* = om översändningen av uppgifterna är i enlighet med nationell lag (omfattas ej av beslut 2008/615/RIF)

9.5 *Bilaga 5 Post typ 1 definitioner*

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{US}15{RS}2{US}00{RS}4 {US}01{RS}4{US}02{RS}4{US}03 {RS}4{US}04{RS}4{US}05{RS}4 {US}06{RS}4{US}07{RS}4{US}08 {RS}4{US}09{RS}4{US}10{RS}4 {US}11{RS}4{US}12{RS}4{US}13 {RS}4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{GS}
DAT	M	1.005	Date	N	1.005:20050101{GS}
PRY	M	1.006	Priority	N	1.006:4{GS}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1.013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Under kolumnen ”Condition”: O = frivillig, M = obligatorisk, C = beroende av tillgängliga uppgifter

Under teckentypkolumn: A = Alfa, N = Numerisk, B = Binär

1* tillåtna tecken för organets namn är [”0...9”, ”A...Z”, ”a...z”, ”_”,”.”, ” ”, ”-”]

9.6 *Bilaga 6 Post typ 2 definitioner*

Tabell A.6.1: CPS- och PMS-transaktion

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

Tabell A.6.2: SRE-Transaktion

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

Tabell A.6.3: ERR-transaktion

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

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC - 1 FIELD 1 009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2 003 INVALID SYSTEM INFORMATION {GS}

Tabell A.6.4: MPS- och MMS-transaktion

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

Under kolumnen ”Condition”: O = frivillig, M = obligatorisk, C = beroende av tillgängliga uppgifter

Under teckentypkolumn: A = Alfa, N = Numerisk, B = Binär

1* tillåtna tecken är [”0...9”, ”A...Z”, ”a...z”, ”_”,”.”, ” ”, ”-”]

9.7 *Bilaga 7 Koder för gråskalekomprimering*

Komprimeringskoder

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 *Bilaga 8 E-postspecifikation*

För att förbättra det interna arbetsflödet måste ärenderubriken för en Prümtransaktion fyllas i med landskod (CC) för den medlemsstat som sänt meddelandet och även typ av transaktion (TOT-fältet 1.004).

Format: CC/*transaktionstyp*

Exempel: ”DE/CPS”

Fältet för meddelandetext kan vara tomt.

KAPITEL 3: **Utbyte av uppgifter i fordonsregister**

1. ***Gemensam uppsättning uppgifter för automatiserad sökning i fordonsregister***

1.1 *Definitioner*

Definitionerna av obligatoriska och frivilliga uppgifter enligt artikel 16.4 är följande:

Obligatoriska uppgifter (M)

Uppgiften måste vidarebefordras när informationen är tillgänglig i en medlemsstats nationella register. Det finns därför en skyldighet att utbyta uppgifterna när de finns tillgängliga.

Frivilliga uppgifter (O)

Uppgiften får vidarebefordras när informationen är tillgänglig i en medlemsstats nationella register. Det finns därför ingen skyldighet att utbyta uppgifterna även om de finns tillgängliga.

Beteckningen (Y) används för varje uppgift i uppsättningen uppgifter som anses vara särskilt viktig med avseende på beslut 2008/615/RIF.

1.2 *Sökning på fordon/ägare/innehavare*

1.2.1 Sökkriterier

Det finns två olika sätt att söka efter uppgifterna, nämligen

— på fordonets identifieringsnummer (VIN), referensdatum och referenstid (frivilliga uppgifter),

— på numret på registreringsskylten, identifieringsnumret (VIN), referensdatum och referenstid (frivilliga uppgifter).

Med hjälp av dessa sökkriterier får man uppgifter om ett eller flera fordon. Om uppgifterna endast gäller ett fordon lämnas samtliga uppgifter i ett svar. Om fler än ett fordon har hittats kan den tillfrågade medlemsstaten själv besluta vilka uppgifter som ska lämnas ut: alla uppgifter eller endast de uppgifter som behövs för att begränsa sökningen (t.ex. av integritetsskäl eller prestandaskäl).

De uppgifter som behövs för att begränsa sökningen anges i punkt 1.2.2.1. I punkt 1.2.2.2 beskrivs den fullständiga uppsättningen uppgifter.

När man söker på identifieringsnummer, referensdatum och referenstid kan sökningen göras i en eller alla deltagande medlemsstater.

När man söker på registreringsnummer, referensdatum och referenstid måste sökningen göras i en viss medlemsstat.

Vanligen används nuvarande datum och tid för sökningen, men det är möjligt att göra en sökning med ett referensdatum och en referenstid i det förflutna. Om man gör en sökning med ett referensdatum och en referenstid i det förflutna, och historiska uppgifter inte finns tillgängliga i en viss medlemsstats register eftersom sådana uppgifter inte registreras över huvud taget, kan de aktuella uppgifterna komma upp som sökresultat med en angivelse om att det rör sig om aktuella uppgifter.

1.2.2 Uppsättning uppgifter

1.2.2.1 Uppgifter som behövs för att begränsa sökningen

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

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

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

1.2.2.2 Fullständig uppsättning uppgifter

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 when available in national register, O = optional.
(2) Harmonised document abbreviation, see Council Directive 1999/37/EC of 29.4.1999.
(3) In Luxembourg two separate vehicle registration document ID's are used.

2. ***Datasäkerhet***

2.1 *Översikt*

Eucaris programapplikation används för säker kommunikation med övriga medlemsstater och kommunicerar med medlemsstaternas äldre back-end-system med hjälp av XML. Medlemsstaterna utbyter meddelanden genom att sända dem direkt till mottagaren. Varje medlemsstats datacentral är ansluten till EU:s Testa-nät.

De XML-meddelanden som sänds via nätet krypteras med krypteringstekniken SSL. De meddelanden som sänds till back-end-systemen är XML-meddelanden i klartext eftersom anslutningen mellan applikationen och back-end-systemen ska vara i en skyddad miljö.

Det tillhandahålls en klientapplikation som kan användas inom en medlemsstat för att söka i dess eget register eller i en annan medlemsstats register. Klienterna identifieras med hjälp av användar-ID/lösenord eller ett klientcertifikat. Anslutningen till en användare kan krypteras, men detta är varje enskild medlemsstats ansvar.

2.2 *Säkerhetsfunktioner i samband med meddelandeutbytet*

Säkerhetssystemet är baserat på en kombination av HTTPS och XML-signatur. Med detta alternativ används XML-signatur för att signera alla meddelanden som sänds till servern, och den som sänder meddelandet kan autentiseras genom att signaturen kontrolleras. Enkelsidig SSL (enbart ett servercertifikat) används för att skydda meddelandets konfidentialitet och integritet under överföringen och skyddar mot raderings-/replay- och insättningsattacker. Istället för skräddarsydd programvaruutveckling för att tillämpa dubbelsidig SSL, tillämpas XML-signatur. Användningen av XML-signatur ligger närmare färdplanen för webbtjänstgränssnitt än dubbelsidig SSL och är därför mer strategisk.

XML-signatur kan tillämpas på flera sätt men man har valt att använda tekniken som en del av *Web Services Security* (WSS). WSS anger hur XML-signatur ska användas. Eftersom WSS bygger på Soap-standarden är det logiskt att följa denna standard så långt det är möjligt.

2.3 *Säkerhetsfunktioner utan samband med meddelandeutbytet*

2.3.1 Autentisering av användare

Användare av Eucaris webbapplikation kan autentisera sig med hjälp av användarnamn och lösenord. Eftersom man använder Windows standardautentisering kan medlemsstaterna vid behov höja autentiseringsnivån för användarna genom att använda klientcertifikat.

2.3.2 Användarroller

Eucaris är anpassad till olika användarroller. Varje grupp av tjänster har en egen behörighetstilldelning. Användare som enbart har behörighet att använda ”Eucarisavtalsfunktionen” får exempelvis inte använda ”Prümfunktionen”. Administratörstjänsterna är avskilda från de vanliga slutanvändarrollerna.

2.3.3 Loggning och spårning av meddelandeutbytet

Eucaris möjliggör loggning av alla typer av meddelanden. Genom en administratörsfunktion kan den nationella administratören bestämma vilka meddelanden som ska loggas: begäranden från slutanvändare, inkommande begäranden från andra medlemsstater, uppgifter som hämtats från de nationella registren osv.

Applikationen kan konfigureras så att den använder en intern databas eller en extern (Oracle) databas för denna loggning. Vilka meddelanden som måste loggas beror naturligtvis på loggningsmöjligheterna i andra delar av de äldre systemen och de anslutna klientapplikationerna.

Rubriken till varje meddelande innehåller information om den begärande medlemsstaten, den begärande organisationen inom den medlemsstaten och den berörda användaren. Skälet till begäran anges också.

Det är möjligt att spåra ett fullständigt meddelandeutbyte (t.ex. på begäran av den berörda medborgaren) med hjälp av den kombinerade loggningen i den begärande och tillfrågade medlemsstaten.

Loggningen konfigureras genom Eucaris webbklient (menu Administration, Logging configuration). Loggningsfunktionen utförs av grundsystemet. När loggningen är aktiverad lagras hela meddelandet (rubriken och meddelandetexten) i en loggningspost. Loggningsnivån kan ställas in enligt angiven tjänst eller enligt den meddelandetyp som passerar genom grundsystemet.

Loggningsnivåer

Följande loggningsnivåer är möjliga:

Privat – meddelandet loggas: Loggen är inte tillgänglig för sökning av loggningar, utan är endast tillgänglig på nationell nivå för revision och problemlösning.

Ingen – meddelandet loggas inte alls.

Typer av meddelanden

Informationsutbytet mellan medlemsstaterna består av flera meddelanden, som illustreras schematiskt i figuren nedan.

De möjliga meddelandetyperna (som i figuren visas för Eucaris grundsystem i medlemsstat X) är följande:

1. Begäran till grundsystemet_meddelande med begäran från klienten
2. Begäran till annan medlemsstat_meddelande med begäran från denna medlemsstats grundsystem
3. Begäran till denna medlemsstats grundsystem_meddelande med begäran från en annan medlemsstats grundsystem
4. Begäran till register i det äldre systemet_meddelande med begäran från grundsystemet
5. Begäran till grundsystemet_meddelande med begäran från register i det äldre systemet
6. Svar från grundsystemet_meddelande med begäran från klienten
7. Svar från annan medlemsstat_meddelande med begäran från denna medlemsstats grundsystem
8. Svar från denna medlemsstats grundsystem_meddelande med begäran från den andra medlemsstaten
9. Svar från register i det äldre systemet_meddelande med begäran från grundsystemet
10. Svar från grundsystemet_meddelande med begäran från register i det äldre systemet

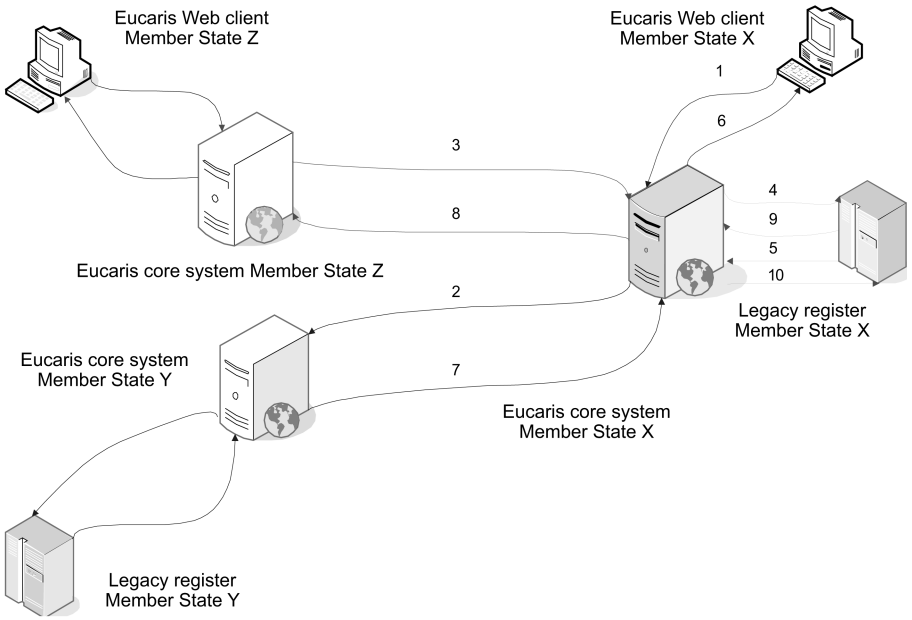
Följande typer av informationsutbyte visas i figuren:

— Begäran om information från medlemsstat X till medlemsstat Y – blå pilar. Denna begäran och svaret består av meddelandetyperna 1, 2, 7 respektive 6.

— Begäran om information från medlemsstat Z till medlemsstat X – röda pilar. Denna begäran och svaret består av meddelandetyperna 3, 4, 9 respektive 8.

— Begäran om information från registret i det äldre systemet till dess grundsystem (detta inkluderar även en begäran från en specialklient bakom registret i det äldre systemet) – gröna pilar. Denna typ av begäran består av meddelandetyperna 5 och 10.

Figur: Meddelandetyper för loggning



2.3.4 Säkerhetsmodul i maskinvara

Ingen säkerhetsmodul används i maskinvaran.

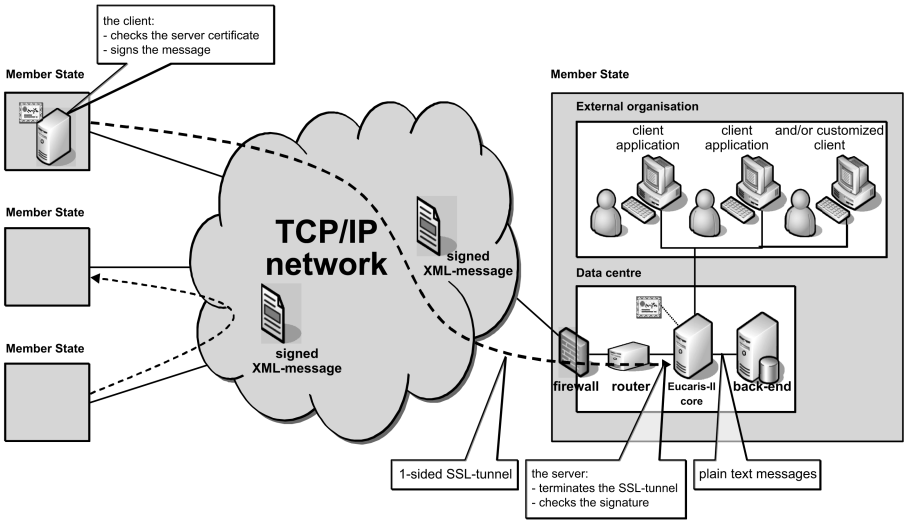
En säkerhetsmodul i maskinvaran (*HSM, Hardware Security Model*) ger ett gott skydd av den nyckel som används för att signera meddelanden och identifiera servrar. Detta bidrar till den allmänna säkerhetsnivån, men kostnaden är hög för inköp/underhåll av en HSM, och det finns inga krav på att använda en HSM som uppfyller nivå 2 eller 3 enligt FIPS-standarden 140-2. Eftersom man använder ett slutet nät som effektivt skyddar mot hot har man beslutat att inledningsvis inte använda någon HSM. Om en HSM blir nödvändig, t.ex. för att ackreditering, kan arkitekturen kompletteras med detta.

3. *Tekniska villkor för informationsutbytet*

3.1 *Allmän beskrivning av Eucaris-applikationen*

3.1.1 Översikt

Eucaris-applikationen kopplar samman alla medlemsstater i ett meshnät där varje medlemsstat kommunicerar direkt med en annan medlemsstat. Ingen central komponent behövs för att etablera kommunikationen. Eucaris-applikationen hanterar säker kommunikation till de andra medlemsstaterna och kommunicerar med back-end-delen i äldre system hos medlemsstater som använder XML. Följande bild visualiserar denna arkitektur.



Medlemsstaterna utbyter meddelanden genom att sända dem direkt till mottagaren. En medlemsstats datacentral är kopplad till det nät som används för utbyte av meddelanden (Testa). För åtkomst av Testa-nätet ansluter sig medlemsstaterna till Testa via sin nationella nätport. En brandvägg ska användas för anslutning till nätet och en router ansluter Eucaris-applikationen till brandväggen. Beroende på vilket alternativ som väljs för att skydda meddelandena, används ett certifikat antingen av routern eller av Eucaris-applikationen.

En klientapplikation tillhandahålls som kan användas inom en medlemsstat för att söka i dess eget register eller andra medlemsstaters register. Klientapplikationen är ansluten till Eucaris. Klienterna identifieras med hjälp av användarID/lösenord eller ett klientcertifikat. Anslutningen till en användare i en extern organisation (t.ex. polisen) kan krypteras men detta är varje enskild medlemsstats ansvar.

3.1.2 Systemets tillämpningsområde

Eucaris-systemets tillämpningsområde är begränsat till processer som används i informationsutbytet mellan registreringsmyndigheterna i medlemsstaterna och en grundläggande presentation av denna information. Förfaranden och automatiserade processer i vilka informationen ska användas faller utanför systemets tillämpningsområde.

Medlemsstater kan välja att antingen använda Eucaris klientfunktion eller skapa sin egen skräddarsydda klientapplikation. I tabellen nedan anges vilka aspekter av Eucaris-systemet som obligatoriskt måste användas och/eller föreskrivs och vilka aspekter som är frivilliga och/eller som medlemsstaterna fritt kan fastställa.

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

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

3.2 *Funktionella och icke funktionella krav*

3.2.1 Generisk funktionalitet

I detta avsnitt har de huvudsakliga generiska funktionerna beskrivits i allmänna termer

Nr	Beskrivning
1.	Systemet gör det möjligt för medlemsstaternas registreringsmyndigheter att utbyta begäranden och svar på ett interaktivt sätt.
2.	Systemet innehåller en klientapplikation som möjliggör för slutanvändare att översända sina begäranden och presentera svarsinformationen för manuell behandling.
3.	Systemet underlättar ”rundsändning”, vilket gör att en medlemsstat kan översända en begäran till alla de övriga medlemsstaterna. De inkommande svaren konsolideras genom grundapplikationen i ett svarsmeddelande till klientapplikationen (denna funktionalitet kallas ”Multiple Country Inquiry”).
4.	Systemet kan hantera olika slags meddelanden. Användarroll, behörighetstilldelning, routing, signering och loggning definieras alla per specifik tjänst.
5.	Systemet gör det möjligt för medlemsstaterna att utbyta meddelanden satsvis eller meddelanden som innehåller ett stort antal begäranden eller svar. Dessa meddelanden behandlas asynkront.
6.	Systemet lägger asynkrona meddelanden i väntekö om den mottagande medlemsstaten tillfälligt inte är tillgänglig och garanterar leveransen så snart som mottagaren är uppkopplad igen.
7.	Systemet lagrar inkommande asynkrona meddelanden tills de kan behandlas.
8.	Systemet ger endast åtkomst till andra medlemsstaters Eucaris-applikationer, inte till individuella organisationer inom dessa andra medlemsstater, vilket innebär att varje registreringsmyndighet agerar som den enda nätporten mellan dess nationella slutanvändare och motsvarande myndigheter i de andra medlemsstaterna.
9.	Det är möjligt att definiera användare från olika medlemsstater på en enda Eucaris-server och att ge dem behörighet i enlighet med gällande bestämmelser i den medlemsstaten.
10.	Meddelandena innehåller också information om den begärande medlemsstaten, organisationen och slutanvändaren.
11.	Systemet underlättar loggning av utbytet av meddelanden mellan de olika medlemsstaterna och mellan huvudapplikationen och de nationella registreringssystemen.
12.	Systemet tillåter att en särskild sekreterare, som är en organisation eller en medlemsstat som explicit har utsetts att sköta denna uppgift, samlar in loggad information om meddelanden som sänts eller mottagits av samtliga deltagande medlemsstater i syfte att sammanställa statistikrapporter.
13.	Varje medlemsstat anger själv vilken loggad information som ska göras tillgänglig för sekreteraren och vilken information som är ”privat”.
14.	Systemet tillåter varje medlemsstats nationella administratörer att ta fram utdrag ur användbar statistik.
15.	Systemet möjliggör tillägg av nya medlemsstater genom enkla administrativa åtgärder.

3.2.2 Användbarhet

Nr	Beskrivning
16.	Systemet tillhandahåller ett gränssnitt för automatiserad behandling av meddelanden med hjälp av back-end-delen i äldre system och möjliggör integration av användargränssnittet i dessa system (skräddarsytt användargränssnitt).
17.	Systemet är lätt att lära sig, självförklarande och innehåller hjälptext.
18.	Systemet är dokumenterat för att bistå medlemsstaterna i fråga om integrering, operativa aktiviteter och framtida underhåll (t.ex. referensmanual, funktionell/operativ dokumentation, användarmanual, ...).
19.	Användargränssnittet är flerspråkigt och erbjuder möjligheter för slutanvändaren att välja ett favoritspråk.
20.	Användargränssnittet tillhandahåller redskap med hjälp av vilka den lokala administratören kan översätta både skärmbildsobjekt och kodad information till det nationella språket.

3.2.3 Tillförlitlighet

Nr	Beskrivning
21.	Systemet är utformat som ett robust och pålitligt operativsystem som tolererar fel som operatören begår och som klarar strömavbrott eller andra olyckor. Det måste vara möjligt att starta om systemet med ingen eller minimal förlust av data.
22.	Systemet måste ge stabila och reproducerbara resultat.
23.	Systemet är utformat så att det fungerar pålitligt. Det är möjligt att implementera systemet i en konfiguration som garanterar 98 % tillgänglighet (genom redundans, användning av backup-servrar, osv.) i all bilateral kommunikation.
24.	Det är möjligt att använda delar av systemet även när några komponenter inte fungerar (om medlemsstat C ligger nere kan fortfarande medlemsstaterna A och B kommunicera). Antalet enskilda felställen i informationskedjan bör minimeras.
25.	Återhämtningstiden efter ett allvarligt haveri bör vara mindre än en dag. Det bör vara möjligt att minimera den tid systemet ligger nere genom användning av fjärrstöd, t.ex. en central servicedesk.

3.2.4 Prestanda

Nr	Beskrivning
26.	Systemet kan användas 24x7. Detta tidsfönster (24x7) krävs då också av medlemsstaternas äldre system.
27.	Systemet reagerar snabbt på en användarbegäran oavsett bakgrundsaktivitet. Detta krävs också av parternas äldre system för att säkerställa en godtagbar svarstid. En total svarstid om maximalt 10 sekunder för en enstaka begäran är godtagbar.
28.	Systemet har utformats som ett fleranvändarsystem och på ett sådant sätt att bakgrundsaktivitet kan fortsätta medan användaren utför förgrundsaktivitet.
29.	Systemet har utformats så att det är skalbart i syfte att klara en potentiell ökning av antalet meddelanden när ny funktionalitet läggs till eller nya organisationer eller medlemsstater ansluter sig.

3.2.5 Säkerhet

Nr	Beskrivning
30.	Systemet lämpar sig (t.ex. beträffande dess säkerhetsåtgärder) för utbyte av meddelanden som innehåller integritetskänslig information (t.ex. bilägare/innehavare) som klassificeras som EU RESTREINT.
31.	Systemet upprätthålls på ett sådant sätt att obehörig åtkomst av information förhindras.
32.	Systemet innehåller en tjänst för hantering av de nationella slutanvändarnas rättigheter och tillstånd.
33.	Medlemsstaterna kan kontrollera sändarens identitet (på medlemsstatsnivå) genom XML-signering.
34.	Medlemsstater måste uttryckligen ge andra medlemsstater behörighet för att de ska kunna begära särskild information.
35.	Systemet tillhandahåller på applikationsnivå en fullständig säkerhets- och krypteringspolicy som är kompatibel med den säkerhetsnivå som krävs i sådana situationer. Informationens exklusivitet och integritet garanteras genom användning av XML-signering och kryptering genom SSL-tunnling.
36.	Allt informationsutbyte kan spåras genom loggning.
37.	Skydd mot raderingsattacker tillhandahålls (en tredje part raderar ett meddelande) och replay- eller insättningsattacker (en tredje part spelar upp eller sätter in ett meddelande).
38.	Systemet använder sig av TTP-certifikat (*Trusted Third Party*).
39.	Systemet kan hantera olika certifikat per medlemsstat beroende på typen av meddelande eller tjänst.

Nr	Beskrivning
40.	Säkerhetsåtgärderna på applikationsnivå är tillräckliga för att tillåta användning av icke ackrediterade nät.
41.	Systemet är förberett för användning av ny säkerhetsteknik såsom en XML-brandvägg.

3.2.6 Anpassbarhet

Nr	Beskrivning
42.	Systemet kan utökas med nya meddelanden och ny funktionalitet. Anpassningskostnaderna är minimala beroende på den centraliserade utvecklingen av applikationskomponenter.
43.	Medlemsstaterna kan definiera nya meddelandetyper för bilateral användning. Det krävs inte av alla medlemsstater att de ska kunna klara av alla typer av meddelanden.

3.2.7 Stöd och underhåll

Nr	Beskrivning
44.	Systemet tillhandahåller övervakningsfaciliteter för en central servicedesk och/eller operatörer när det gäller nätet och servrar i de olika medlemsstaterna.
45.	Systemet tillhandahåller faciliteter för fjärrstöd genom en central servicedesk.
46.	Systemet tillhandahåller faciliteter för problemanalys.
47.	Systemet kan utsträckas till att omfatta nya medlemsstater.
48.	Applikationen kan enkelt installeras av personal med ett minimum av IT-kvalifikationer och erfarenhet. Installationsproceduren ska så långt som möjligt vara automatiserad.
49.	Systemet tillhandahåller en permanent test- och acceptansmiljö.
50.	De årliga kostnaderna för underhåll och stöd har minimerats genom anslutning till marknadsstandarder och genom att utforma applikationen så att så lite stöd som möjligt krävs från en central servicedesk.

3.2.8 Krav på utformningen

Nr	Beskrivning
51.	Systemet är utformat och dokumenterat för en operativ livslängd på många år.
52.	Systemet har utformats så att det är oberoende av nätleverantören.
53.	Systemet står i överensstämmelse med existerande HW/SW i medlemsstaterna genom att interagera med de registreringssystem som använder öppna standarder för webbtjänstteknik (XML, XSD, Soap, WSDL, HTTP(s), webbtjänster, WSS, X.509, osv.).

3.2.9 Tillämpliga standarder

Nr	Beskrivning
54.	Systemet uppfyller dataskyddskraven i förordning (EG) nr 45/2001 (artiklarna 21, 22 och 23) och direktiv 95/46/EG.
55.	Systemet uppfyller IDA-standarderna.
56.	Systemet är anpassat för UTF8.

KAPITEL 4: **Utvärdering**

1. ***Utvärderingsförfarande i enlighet med artikel 20 (förberedelse av beslut enligt artikel 25.2 i beslut 2008/615/RIF)***

1.1 *Frågeformulär*

Den berörda rådsarbetsgruppen ska utarbeta ett frågeformulär beträffande vart och ett av de automatiserade utbytena av information i kapitel 2 i beslut 2008/615/RIF.

Så snart som en medlemsstat anser sig uppfylla de nödvändiga förutsättningarna för att dela information i de relevanta informationskategorierna ska den besvara det relevanta frågeformuläret.

1.2 *Testkörning*

I syfte att utvärdera resultatet av frågeformuläret ska de medlemsstater som vill börja dela information genomföra en testkörning tillsammans med en eller flera andra medlemsstater som redan delar information enligt rådsbeslutet. Testkörningen ska äga rum före eller kort tid efter utvärderingsbesöket.

Villkoren och arrangemangen kring denna testkörning ska fastställas av den berörda rådsarbetsgruppen och grunda sig på en i förväg träffad separat överenskommelse med den berörda medlemsstaten. De medlemsstater som deltar i testkörningen beslutar själva om de praktiska detaljerna.

1.3 *Utvärderingsbesök*

I syfte att utvärdera resultatet av frågeformuläret ska ett utvärderingsbesök äga rum i den medlemsstat som vill börja dela information.

Villkoren och arrangemangen kring denna testkörning kommer att fastställas av den berörda rådsarbetsgruppen och grunda sig på en i förväg träffad separat överenskommelse mellan den berörda medlemsstaten och utvärderingsteamet. Den berörda medlemsstaten ska ge utvärderingsteamet möjlighet att kontrollera det automatiserade informationsutbytet i den eller de informationskategorier som ska utvärderas, bland annat genom att organisera ett program för besöket som beaktar de önskemål som utvärderingsteamet framfört.

Inom en månad ska utvärderingsteamet sammanställa en rapport om utvärderingsbesöket och överlämna den till berörda medlemsstater för kommentarer. I förekommande fall ska utvärderingsgruppen revidera denna rapport på grundval av medlemsstaternas kommentarer.

Utvärderingsteamet ska bestå av högst tre experter, utsedda av de medlemsstater som deltar i det automatiserade informationsutbytet i de informationskategorier som ska utvärderas, som har erfarenhet beträffande den berörda informationskategorin, som har genomgått lämplig nationell säkerhetskontroll för att få handha dessa frågor och som är villiga att delta i åtminstone ett utvärderingsbesök i en annan medlemsstat.

Medlemmarna i utvärderingsteamet ska respektera den inhämtade informationens konfidentiella natur i samband med att de utför sin uppgift.

1.4 *Rapport till rådet*

En övergripande utvärderingsrapport som sammanfattar resultatet av frågeformulären, utvärderingsbesöket och testkörningen kommer att läggas fram för rådet för beslut i enlighet med artikel 25.2 i beslut 2008/615/RIF.

2. ***Utvärderingsförfarande enligt artikel 21***

2.1 *Statistik och rapport*

Varje medlemsstat ska samla in statistik över resultatet av det automatiserade informationsutbytet. I syfte att säkerställa jämförbarhet kommer statistikmodellen att fastställas av den berörda rådsarbetsgruppen.

Dessa statistikuppgifter kommer årligen att läggas fram för rådet, som ska göra en övergripande sammanfattning av det gångna året, och för kommissionen.

Dessutom kommer medlemsstaterna regelbundet att anmodas att inte underlåta att en gång per år tillhandahålla sådana ytterligare uppgifter om det administrativa, tekniska och finansiella genomförandet av automatiserat utbyte av information som behövs för analys och förbättringar av processen. På grundval av denna information kommer en rapport att sammanställas för rådet.

2.2 *Revidering*

Inom rimlig tid kommer rådet att granska den utvärderingsmekanism som beskrivs här och vid behov revidera den.

3. Expertmöten

Inom den berörda rådsarbetsgruppen kommer experter regelbundet att träffas för att organisera och genomföra de ovannämnda utvärderingsförfarandena samt dela med sig av sina erfarenheter och diskutera möjliga förbättringar. I tillämpliga fall kommer resultatet av dessa expertdiskussioner att införlivas med den rapport som det hänvisas till i punkt 2.1 ovan.

RÅDETS BESLUT 2008/617/RIF

av den 23 juni 2008

om förbättrat samarbete i krissituationer mellan Europeiska unionens medlemsstaters särskilda insatsgrupper

EUROPEISKA UNIONENS RÅD HAR BESLUTAT FÖLJANDE

med beaktande av fördraget om Europeiska unionen, särskilt artiklarna 30, 32 och 34.2 c,

med beaktande av Republiken Österrikes initiativ ([1]),

med beaktande av Europaparlamentets yttrande ([2]), och

av följande skäl:

(1) Enligt artikel 29 i fördraget ska unionens mål vara att ge medborgarna en hög säkerhetsnivå inom ett område med frihet, säkerhet och rättvisa genom att bland medlemsstaterna utforma gemensamma insatser på områdena polissamarbete och straffrättsligt samarbete.

(2) Europeiska unionens medlemsstaters stats- och regeringschefer förklarade i sitt uttalande av den 25 mars 2004 om solidaritet i kampen mot terrorismen att det var deras bestämda avsikt att medlemsstaterna ska mobilisera alla instrument som står till deras förfogande för att i händelse av en terroristattack bistå en medlemsstat eller en anslutande stat på dess territorium på begäran av dess politiska myndigheter.

(3) Med anledning av attackerna den 11 september 2001 har de särskilda insatsgrupperna inom alla brottsbekämpande organ i medlemsstaterna redan inlett samarbete under överinseende av den operativa specialgruppen med polischefer. Detta nätverk, kallat Atlas, har genomfört diverse seminarier, studier, utbyten av material och gemensamma övningar sedan 2001.

(4) Ingen medlemsstat förfogar själv över alla de medel och resurser och den expertis som behövs för att effektivt hantera alla möjliga typer av bestämda eller storskaliga krissituationer där det krävs särskilda insatser. Det är därför av avgörande betydelse att varje medlemsstat kan begära bistånd av en annan medlemsstat.

(5) Rådets beslut 2008/615/RIF av den 23 juni 2008 om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet ([3]) (Prümbeslutet), och särskilt artikel 18 i det beslutet, reglerar formerna för polisärt bistånd mellan medlemsstaterna vid större evenemang och liknande viktiga händelser, vid katastrofer och vid allvarliga olyckor. Detta beslut omfattar inte större evenemang, naturkatastrofer eller allvarliga olyckor i enlighet med artikel 18 i Prümbeslutet, utan utgör en komplettering av de bestämmelser i Prümbeslutet som möjliggör former av polisärt bistånd mellan medlemsstaterna genom särskilda insatsgrupper i andra situationer, dvs. krissituationer som är förorsakade av människor och som innebär ett allvarligt direkt fysiskt hot mot personer, egendom, infrastruktur eller institutioner, särskilt tagande av gisslan, kapning och liknande händelser.

(6) När denna ram och en sammanställning där de behöriga myndigheterna anges finns tillgängliga kommer det att bli möjligt för medlemsstaterna att reagera snabbt och vinna tid om en sådan krissituation inträffar. I syfte att förbättra medlemsstaternas förmåga att förhindra och åtgärda sådana krissituationer är det vidare viktigt att de särskilda insatsgrupperna träffas regelbundet och anordnar gemensam utbildning för att dra fördel av varandras erfarenheter.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

I detta beslut fastställs allmänna regler och villkor som möjliggör att en medlemsstats särskilda insatsgrupper lämnar bistånd och/eller opererar på en annan medlemsstats territorium i sådana fall där de blivit ombedda av den andra medlemsstaten (nedan kallad *den ansökande medlemsstaten*) och har samtyckt till att göra detta för att hantera en krissituation. De praktiska detaljer och genomförandebestämmelser som kompletterar detta beslut ska fastställas direkt i samråd mellan den ansökande medlemsstaten och den anmodade medlemsstaten.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner:

a) *särskild insatsgrupp*: varje brottsbekämpande enhet i en medlemsstat, vilken har hantering av krissituationer som en specialuppgift.

([1]) EUT C 321, 29.12.2006, s. 45.
([2]) Yttrandet avgivet den 31 januari 2008 (ännu ej offentliggjort i EUT).
([3]) Se sidan 1 i detta nummer av EUT.

b) *krissituation*: varje situation i en medlemsstat där de behöriga myndigheterna i en medlemsstat har rimlig anledning att förmoda att det föreligger ett brott som innebär ett allvarligt direkt fysiskt hot mot personer, egendom, infrastruktur eller institutioner i den medlemsstaten, särskilt sådana situationer som avses i artikel 1.1 i rådets rambeslut 2002/475/RIF av den 13 juni 2002 om bekämpande av terrorism ([1]).

c) *behörig myndighet*: den nationella myndighet som får göra ansökningar om eller bemyndiga användning av de särskilda insatsgrupperna.

Artikel 3

Bistånd till en annan medlemsstat

1. Genom en begäran via de behöriga myndigheterna, i vilken det begärda biståndets art och det operativa behovet av bistånd anges, kan en medlemsstat begära att få bistånd av en särskild insatsgrupp i en annan medlemsstat för att hantera en krissituation. Den anmodade medlemsstatens behöriga myndighet får fritt besluta att bevilja eller avslå en sådan begäran eller föreslå någon annan typ av bistånd.

2. Med förbehåll för en överenskommelse mellan de berörda medlemsstaterna kan biståndet bestå av tillhandahållande av utrustning och/eller expertis till den ansökande medlemsstaten och/eller av genomförande av operationer på den medlemsstatens territorium, om så krävs med användning av vapen.

3. När det gäller operationer på den ansökande medlemsstatens territorium ska tjänstemännen i den bistående särskilda insatsgruppen bemyndigas att agera i en stödfunktion på den ansökande medlemsstatens territorium och vidta alla de åtgärder som är nödvändiga för att lämna det begärda biståndet förutsatt att de

a) opererar på den ansökande medlemsstatens ansvar, under dess bemyndigande och ledning samt i enlighet med den ansökande medlemsstatens lagstiftning, och

b) opererar inom ramen för sina befogenheter enligt sitt lands nationella lagstiftning.

Artikel 4

Civilrättsligt och straffrättsligt ansvar

När tjänstemän från en medlemsstat opererar i en annan medlemsstat och/eller utrustning används i enlighet med detta beslut ska de regler om civilrättsligt och straffrättsligt ansvar som anges i artiklarna 21.4, 21.5 och 22 i Prümbeslutet gälla.

([1]) EGT L 164, 22.6.2002, s. 3.

Artikel 5

Möten och gemensam utbildning

De deltagande medlemsstaterna ska se till att deras särskilda insatsgrupper håller möten och anordnar gemensam utbildning och gemensamma övningar närhelst det är nödvändigt, i syfte att utbyta erfarenheter och expertis samt allmän, praktisk och teknisk information om sätt att hantera en krissituation. Mötena, utbildningen och övningarna får finansieras genom de möjligheter att beviljas anslag ur Europeiska unionens budget som erbjuds genom unionens finansiella program. I detta sammanhang ska den medlemsstat som innehar unionens ordförandeskap sträva efter att säkerställa att denna utbildning och dessa möten och övningar äger rum.

Artikel 6

Kostnader

Den ansökande medlemsstaten ska ansvara för de driftskostnader som den anmodade medlemsstatens särskilda insatsgrupper ådrar sig i samband med tillämpningen av artikel 3, inbegripet kostnader för transport och förläggning, om inte de berörda medlemsstaterna har kommit överens om någonting annat.

Artikel 7

Förhållandet till andra instrument

1. Medlemsstaterna får utan att det påverkar deras åtaganden enligt andra rättakter som antagits enligt avdelning VI i fördraget, särskilt Prümbeslutet

a) fortsätta att tillämpa bilaterala eller multilaterala avtal eller överenskommelser om gränsöverskridande samarbete som är i kraft den 23 juni 2008, förutsatt att dessa avtal eller överenskommelser inte är oförenliga med målen för detta beslut,

b) ingå eller låta träda i kraft bilaterala eller multilaterala avtal eller överenskommelser om gränsöverskridande samarbete efter den 23 december 2008, förutsatt att dessa avtal eller överenskommelser gör det möjligt att utvidga eller bredda målen för detta beslut.

2. De avtal och överenskommelser som avses i punkt 1 får inte påverka förbindelserna med de medlemsstater som inte är parter i dem.

3. Medlemsstaterna ska underrätta rådet och kommissionen om sådana avtal och överenskommelser som avses i punkt 1.

Artikel 8

Slutbestämmelser

Rådets generalsekretariat ska sammanställa och kontinuerligt uppdatera förteckningen över de behöriga myndigheter i medlemsstaterna som får göra ansökningar om eller bemyndiga lämnande av bistånd enligt artikel 3.

Rådets generalsekretariat ska underrätta de myndigheter som nämns i punkt 1 om varje förändring i den förteckning som upprättats i enlighet med denna artikel.

Artikel 9

Ikraftträdande

Detta beslut träder i kraft den 23 december 2008.

Utfärdat i Luxemburg den 23 juni 2008.

På rådets vägnar

I. JARC

Ordförande