RÅDET FOR DEN EUROPÆISKE UNION

Bruxelles, den 26. marts 2008 (31.03)
(OR. en)

7713/08

CRIMORG 52
ENFOPOL 54

NOTE

fra:	formandskabet
til:	delegationerne
Tidl. dok. nr.:	5660/08 CRIMORG 18 ENFOPOL 21
Vedr.:	Udkast til Rådets afgørelse om gennemførelse af afgørelse 2008/.../RIA om intensivering af det grænseoverskridende samarbejde, navnlig om bekæmpelse af terrorisme og grænseoverskridende kriminalitet: Bilaget – Resultat af drøftelserne

1. Artikel 36-Udvalget nåede den 6. februar 2008 til enighed om teksten til bilaget til ovennævnte rådsafgørelse som gengivet i bilaget til denne note, jf. dog visse undersøgelsesforbehold.

2. De pågældende delegationer har i mellemtiden meddelt, at de kan hæve disse forbehold.

3. Som følge heraf vil afgørelsen om gennemførelse af Prümaftalen (dok. 16239/07 CRIMORG 188 ENFOPOL 217) inklusive bilaget til denne note blive forelagt Coreper og Rådet, så snart Europa-Parlamentet har afgivet udtalelse i begyndelsen af april.

BILAG

INDHOLD

9. Tillæg til kapitel 2
   - 9.1 ASCII Separatorkoder
   - 9.2 Beregning af alfanumeriske kontroltegn
   - 9.3 Tegnkoder
   - 9.4 Transaktionsresumé
   - 9.5 Definitioner i type-1 record
   - 9.6 Definitioner af type-2 records
   - 9.7 Gråtonekompressionskoder
   - 9.8 Mailspecification

Kapitel 3: Udveksling af oplysninger fra køretøjsregistre

1. Fælles data med henblik på elektronisk søgning af oplysninger fra køretøjsregistre
   - 1.1 Definitioner
   - 1.2 Søgen efter køretøj/ejer/bruger
2. Datasikkerhed
   - 2.1 Oversigt
   - 2.2 Sikkerhedsfeatures i forbindelse med udveksling af meddelelser
   - 2.3 Sikkerhedsfeatures uden forbindelse med udveksling af meddelelser
3. De tekniske betingelser for dataudvekslingen
   - 3.1 Generel beskrivelse af Eucarisprogrammet
   - 3.2 Funktionelle og ikke-funktionelle krav

Kapitel 4: Evaluering

1. Evalueringsprocedure i henhold til artikel 20 (Forberedelse af afgørelser omhandlet i artikel 25, stk. 2, i afgørelse 2008/.../RIA)
   - 1.1 Spørgeskema
   - 1.2 Forsøgsfase
   - 1.3 Evalueringsbesøg
   - 1.4 Rapport til Rådet
2. Evalueringsprocedure i henhold til artikel 21
   - 2.1 Statistikker og rapport
   - 2.2 Revision
3. Ekspertmøder

Kapitel 1: Udveksling af dna-oplysninger

1. Dna-relaterede retsmedicinske spørgsmål, overensstemmelsesregler og algoritmer

1.1 Egenskaber ved dna-profilerne

Dna-profilen kan indeholde 24 talpar, der repræsenterer allelerne af 24 loci, der også benyttes i Interpols dna-procedurer. Navnene på disse loci er anført i følgende skema:

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 7 grå loci i øverste række er det nuværende europæiske standardsæt (ESS) og Interpols standardsæt af loci (ISSOL).

Medtagelsesregler:

De dna-profiler, som medlemsstaterne stiller til rådighed for eller udsender med henblik på søgning og sammenligning, skal indeholde mindst 6 fulde udpegede[1] loci og kan indeholde yderligere loci eller blanke felter alt efter, hvad der er tilgængeligt. Reference-dna-profilerne skal indeholde mindst 6 af de 7 ESS-loci. For at højne overensstemmelsespræcisionen opbevares alle de tilgængelige alleler i den indekserede dna-profildatabase og benyttes til søgning og sammenligning. Hver medlemsstat bør, så hurtigt som det er praktisk gennemførligt, implementere enhver ny ESS for loci, som vedtages af EU.

Blandede profiler er ikke tilladt, hvilket vil sige, at allelværdien for hvert locus kun består af 2 tal, der kan være ens i tilfælde af homozygositet i et givet locus.

Jokere og mikrovarianter behandles efter følgende regler:

- Enhver ikke-numerisk værdi bortset fra amelogenin i profilen (f.eks. "o", "f", "r", "na", "nr" eller "un") skal ved eksport automatisk konverteres til en joker (*) og søges på i forhold til alle.
- Numeriske værdier "0", "1" eller "99" i profilen skal ved eksport automatisk konverteres til en joker (*) og søges på i forhold til alle.

[1] "Fulde udpegede" betyder, at behandlingen af sjældne allelværdier er medtaget.

Hvis der forekommer 3 alleler for en og samme locus, vil det første allel blive accepteret, og de 2 andre alleler skal ved eksport automatisk konverteres til en joker (*) og søges på i forhold til alle.

- Når der forekommer jokerværdier for allel 1 eller 2, vil der blive søgt på begge permutationer af den numeriske værdi for den pågældende locus (f.eks. vil 12, * give overensstemmelse med 12,14 eller 9,12).

- Pentanucleotide (Penta D, Penta E & CD4) mikrovarianter vil give overensstemmelse efter følgende model:

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

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

x.3 = x.2, x.3, x.4

x.4 = x.3, x.4, x+1

- Tetranucleotide (alle andre loci er tetranucleotide) mikrovarianter vil give overensstemmelse efter følgende model:

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

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

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

1.2 Overensstemmelsesregler

Sammenligningen af to dna-profiler sker på grundlag af de loci, for hvilke et allelværdipar er til stede i begge dna-profiler. Mindst 6 fulde udpegede loci (ekskl. amelogenin) skal være sammenfaldende i de to dna-profiler, før der gives overensstemmelsessvar.

Fuld overensstemmelse (kvalitet 1) defineres som en overensstemmelse, hvor alle allelværdier for de sammenlignede loci, der er almindeligt forekommende i de anmodende og anmodede dna-profiler, er ens. Næsten-overensstemmelse defineres som en overensstemmelse, hvor kun værdien af en enkelt af alle de sammenlignede alleler er forskellig i de to dna-profiler (kvalitet 2, 3 og 4). En næsten-overensstemmelse accepteres kun, hvis der er mindst 6 fulde udpegede overensstemmende loci i de to sammenlignede dna-profiler.

En næsten-overensstemmelse kan skyldes:

- En menneskelig slåfejl i en af dna-profilerne i søgningen eller dna-databasen ved indrejsestedet,
- en allelbestemmelses- eller allelfremkaldelsesfejl under genereringen af dna-profilen.

1.3 Indberetningsregler

Både fuld overensstemmelse, næsten-overensstemmelse og "ingen overensstemmelse" vil blive indberettet.

Overensstemmelsesrapporten vil blive sendt til det anmodende nationale kontaktpunkt og gøres også tilgængelig for det anmodede nationale kontaktpunkt (så det kan danne sig et overblik over, hvor mange og hvilke typer opfølgende anmodninger, der vil kunne komme om yderligere tilgængelige personoplysninger og andre oplysninger vedrørende den dna-profil, der svarer til den fundne overensstemmelse jf. artikel 5 og 10 i afgørelse 2008/.../RIA.

2. Skema over medlemsstaternes landekoder

I overensstemmelse med afgørelse 2008/.../RIA, benyttes ISO 3166-1 alpha-2 koderne til domænenavne og andre konfigureringsparametre, der er krævet i Prümaftalens dna-udvekslingsprogrammer via et lukket netværk.

ISO 3166-1 alpha-2 koderne for medlemsstaterne er nedenstående landekoder med to bogstaver.

Medlemsstaternes navne	**Kode**	**Medlemsstaternes navne**	**Kode**
Belgien	BE	Luxembourg	LU
Bulgarien	BG	Ungarn	HU
Den Tjekkiske Republik	CZ	Malta	MT
Danmark	DK	Nederlandene	NL
Tyskland	DE	Østrig	AT
Estland	EE	Polen	PL
Grækenland	EL	Portugal	PT
Spanien	ES	Rumænien	RO
Frankrig	FR	Slovakiet	SK
Irland	IE	Slovenien	SI
Italien	IT	Finland	FI
Cypern	CY	Sverige	SE
Letland	LV	Det Forenede Kongerige	UK
Litauen	LT		

3. Funktionsanalyse

3.1 Systemets tilgængelighed

Anmodninger i henhold til artikel 3 i afgørelse 2008/.../RIA bør nå frem til den søgte database i kronologisk orden efter de enkelte anmodningers afsendelsestidspunkt, og svarene bør afsendes, så de når frem til den anmodende medlemsstat senest 15 minutter efter, at anmodningen er modtaget.

3.2 Anden etape

Når en medlemsstat modtager en indberetning om overensstemmelse er dens nationale kontaktpunkt ansvarlig for at sammenligne værdierne i den profil, der blev indsendt som en forespørgsel, med værdierne i den eller de profiler, der blev modtaget som svar, med henblik på at validere og kontrollere profilens beviskraft. De nationale kontaktpunkter kan kontakte hinanden direkte om spørgsmål, der vedrører validering.

De juridiske bistandsprocedurer starter efter valideringen af en konstateret overensstemmelse mellem to profiler, på grundlag af en "fuld overensstemmelse" eller en "næsten-overensstemmelse", der er fremkommet under den automatiske konsultationsfase.

4. Dna-grænsefladekontroldokumentet (ICD)

4.1 Indledning

4.1.1 Formål

I dette kapitel defineres kravene vedrørende udveksling af dna-profiloplysninger mellem alle medlemsstaternes dna-databasesystemer. Headerfelterne er defineret specielt med henblik på Prüm-udvekslingen af dna-oplysninger, og datadelen er baseret på dna-profildatadelen i det XML-skema, der er defineret til Interpols dna-udvekslingsgateway.

Oplysningerne udveksles med SMTP (Simple Mail Transfer Protocol) og andre avancerede teknologier og benytter en central relay mail server, som netudbyderen stiller til rådighed. XML-filen sendes som mail body.

4.1.2 Anvendelsesområde

Dette ICD definerer kun indholdet af meddelelsen (mailen). Alle netværksspecifikke og mailspecifikke elementer er defineret ens, så der opnås et fælles teknisk grundlag for udvekslingen af dna-oplysninger.

Dette omfatter:

- Formatet af meddelelsens emnefelt, så det bliver muligt at edb-behandle meddelelserne,
- overvejelser om behovet for kryptering, og i bekræftende fald, hvilke metoder der bør vælges,
- meddelelsernes maksimale længde.

4.1.3 XML-struktur og principper

XML-meddelelsen er opdelt i

- en headerdel, der indeholder oplysninger om transmissionen, og
- en datadel, der indeholder profilspecifikke oplysninger samt selve profilen.

Det samme XML-skema benyttes til anmodning og til svar.

Når det drejer sig om komplette verifikationer af uidentificerede dna-profiler (artikel 4 i afgørelse 2008/.../RIA), skal det være muligt at sende flere profiler i samme meddelelse. Der skal fastsættes et maksimalt antal profiler, der kan være indeholdt i en enkelt meddelelse. Antallet vil afhænge af den maksimale størrelse, en mail må have, og skal fastlægges, når valget af mailserver er foretaget.

XML-eksempel:

<?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 gentages, hvis flere profiler sendes i
(....) en og samme SMTP-meddelelse, kun tilladt i artikel 4-tilfælde
</datas>]
</PRUEMDNA>

4.2 Definition af XML-strukturen

Definitionerne i det følgende tjener kun dokumentationsformål og til at forbedre læsbarheden. De egentlige bindende oplysninger findes i en XML-skema-fil (PRUEM DNA.xsd).

4.2.1 Skemaet PRUEMDNAx

Det indeholder følgende felter:

Fields	Type	Description
header	PRUEM_header	Occurs: 1
data	PRUEM_data	Occurs: 1 … 500

4.2.2 Indholdet af headerstrukturen

4.2.2.1 PRUEM header

Denne struktur beskriver XML-filens header. Den indeholder følgende felter:

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

Type data i meddelelsen. Værdien kan være:

Value	Description
R	Request
A	Answer

4.2.2.3 PRUEM header info

Denne struktur beskriver medlemsstaten samt dato og tidspunkt. Den indeholder følgende felter:

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. Indholdet af PRUEM-profilens data

4.2.3.1 PRUEM_datas

Denne struktur beskriver XML-profilens datadel. Den indeholder følgende felter:

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

Typer af data i meddelelsen. Værdien kan være:

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

Typer af data i meddelelsen. Værdien kan være:

Value	Description
P	Person profile
S	Stain

4.2.2.5 PRUEM_data_result

Typer af data i meddelelsen. Værdien kan være:

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

4.2.3.6 IPSG_DNA_profile

Denne struktur beskriver en dna-profil. Den indeholder følgende felter:

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

Denne struktur indeholder ISSOL-loci (Standard Group of Interpol loci). Den indeholder følgende felter:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogin

4.2.3.8 IPSG_DNA_additional_loci

Denne struktur indeholder de øvrige loci. Den indeholder følgende felter:

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

Denne struktur beskriver en locus. Den indeholder følgende felter:

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

5. Program, sikkerhed og kommunikationsarkitektur

5.1 Oversigt

Når der implementeres programmer til dna-udveksling inden for rammerne af afgørelse 2008/.../RIA, skal der benyttes et fælles kommunikationsnetværk, der vil blive logisk lukket til medlemsstaternes kreds. For at udnytte denne fælles kommunikationsinfrastruktur til afsendelse af anmodninger og modtagelse af svar så effektivt som muligt, anvendes en asynkron mekanisme til transmission af anmodninger om dna-oplysninger og fingeraftryksoplysninger i en "wrapped" SMTP-e-mail. Af hensyn til sikkerheden vil SMTP-funktionen blive suppleret med S/MIME-mekanismen for at skabe en veritabel sikker ende-til-ende tunnel via netværket.

De operationelle TESTA (**T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations) anvendes som kommunikationsnet for udvekslingen af oplysninger mellem medlemsstaterne. TESTA fungerer under Europa-Kommissionens ansvar. I betragtning af, at de nationale dna-databaser og det nuværende nationale TESTA-tilkoblingspunkt kan befinde sig på forskellige operationssteder i medlemsstaterne, kan adgangen til TESTA etableres enten ved at:

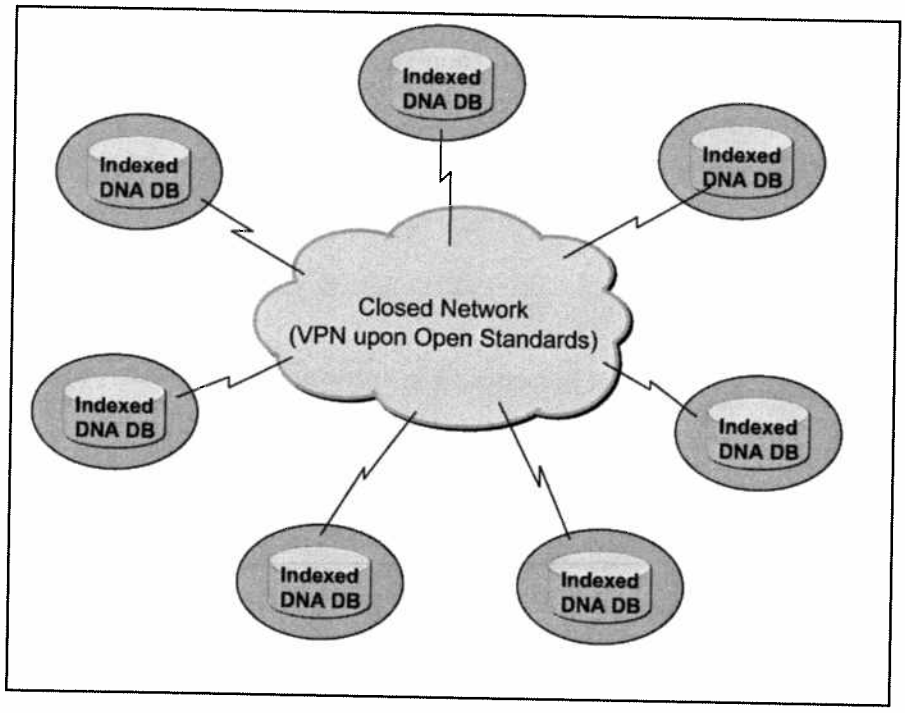
1) benytte det nuværende nationale tilkoblingspunkt eller oprette et nyt nationalt tilkoblingspunkt til TESTA, eller ved at
2) oprette et sikkert lokalt link fra det operationssted, hvor dna-databasen befinder sig og forvaltes af det kompetente nationale agentur, til det nuværende nationale tilkoblingspunkt til TESTA.

Protokollerne og standarderne i de programmer, der benyttes ved gennemførelsen af afgørelse 2008/.../RIA, er i overensstemmelse med de åbne standarder og opfylder de krav, som medlemsstaternes nationale sikkerhedspolitiske beslutningstagere har opstillet.

5.2 Den overordnede arkitektur

I medfør af afgørelse 2008/.../RIA stiller hver medlemsstat sine dna-oplysninger til rådighed for udveksling med andre medlemsstater og/eller for andre medlemsstaters søgning i dem under overholdelse af det standardiserede fælles dataformat. Arkitekturen er baseret på en alle-til-alle kommunikationsmodel. Der findes hverken en central computerserver eller en centraliseret database, hvor dna-profilerne opbevares.

Fig. 1: Skematisk oversigt over udvekslingen af dna-oplysninger



Foruden at opfylde de nationale juridiske krav på medlemsstaternes operationssteder, kan hver medlemsstat desuden beslutte, hvilken type hardware og software der skal benyttes ved konfigureringen på operationsstedet med henblik på at opfylde kravene i afgørelse 2008/.../RIA.

5.3 Sikkerhedsstandarder og databeskyttelse

Der er blevet drøftet og indført sikkerhedsforanstaltninger på tre niveauer.

5.3.1 Dataniveauet

De dna-profildata, som de enkelte medlemsstater leverer, skal forberedes i overensstemmelse med en fælles databeskyttelsesstandard, så de anmodende medlemsstater modtager et svar, der først og fremmest angiver, om der er overensstemmelse eller ej, samt i tilfælde af overensstemmelse et identifikationsnummer, der ikke indeholder nogen personoplysninger. Den videre efterforskning efter meddelelsen om en overensstemmelse sker på bilateralt plan efter de respektive medlemsstaters operationssteders gældende nationale juridiske og organisatoriske regler.

5.3.2 Kommunikationsniveauet

Meddelelser, der indeholder dna-profiloplysninger (anmodninger og svar) krypteres ved hjælp af en avanceret mekanisme efter åbne standarder, såsom S/MIME, inden de sendes til de andre medlemsstaters operationssteder.

5.3.3 Transmissionsniveauet

Alle krypterede meddelelser, der indeholder dna-profiloplysninger, sendes til andre medlemsstaters operationssteder via et virtuelt, privat tunnelsystem, der administreres af en betroet netværksudbyder i international kontekst og via de sikre forbindelser til dette tunnelsystem, der er underlagt medlemsstatens nationale ansvar. Dette virtuelle private tunnelsystem har ingen kontaktflader med det åbne internet.

5.4. Protokoller og standarder, der skal benyttes til krypteringsmekanismen: S/MIME og dertil hørende pakker

De facto e-mail-standarden SMTP vil blive suppleret med open standard-programmet S/MIME med henblik på krypteringen af meddelelser, der indeholder dna-profil-oplysninger. S/MIME-protokollen (V3) muliggør signerede kvitteringer, sikkerhedsmærkninger og sikre mailing-lister og er baseret på Cryptographic Message Syntax (CMS), en IETF-specifikation for kryptografisk beskyttede meddelelser. Den kan benyttes til digital underskrift, digitalt fingeraftryk, autentificering eller kryptering af enhver form for digitale data.

Det underliggende certifikat, som S/MIME benytter, skal være i overensstemmelse med X.509-standarden. Med henblik på at sikre, at de samme standarder og procedurer også gælder for andre Prüm-programmer, er behandlingsreglerne for S/MIME-krypteringsoperationer eller behandlingsreglerne i forbindelse med diverse COTS (Commercial Product of the Shelves)-miljøer som følger:

- Operationernes rækkefølge er: først kryptering og derefter signatur.
- Krypteringsalgoritmen AES (Advanced Encryption Standard) med en nøglestørrelse på 256 bit og RSA med en nøglestørrelse på 1024 bit skal benyttes ved henholdsvis symmetrisk og asymmetrisk kryptering.
- Hash-algoritmen SHA-1 skal benyttes.

S/MIME funktionaliteten er indbygget i de langt de fleste moderne e-mail-programmer, herunder Outlook, Mozilla Mail og Netscape Communicator 4.x, og den kan kombineres med alle de mest fremtrædende e-mail-softwarepakker.

Fordi S/MIME er så let at integrere i de nationale it-infrastrukturer på alle medlemsstaternes operationssteder, er den valgt som en brugbar mekanisme til at implementere kommunikationssikkerhedsniveauet. For at opnå målsætningen om "Proof of Concept" på en mere effektiv måde og for at reducere omkostningerne, har man imidlertid valgt open standard-programmet JavaMail API til prototypen for udveksling af dna-oplysninger. JavaMail API foretager en simpel kryptering og afkryptering af e-mails ved hjælp af S/MIME og/eller OpenPGP. Hensigten er at stille en enkel, brugervenlig API til rådighed for e-mail-brugere, der ønsker at sende og modtage krypteret e-mail i et af de to mest populære e-mail-krypteringsformater. Derfor vil en hvilken som helst avanceret implementering til JavaMail API være tilstrækkelig til at opfylde kravene i afgørelse 2008/.../RIA, som f.eks. Bouncy Castle JCE's produkt **J**ava **C**ryptographic **E**xtension, der vil blive benyttet til at indføre S/MIME i prototypen for udveksling af dna-oplysninger mellem alle medlemsstaterne.

5.5 Programarkitektur

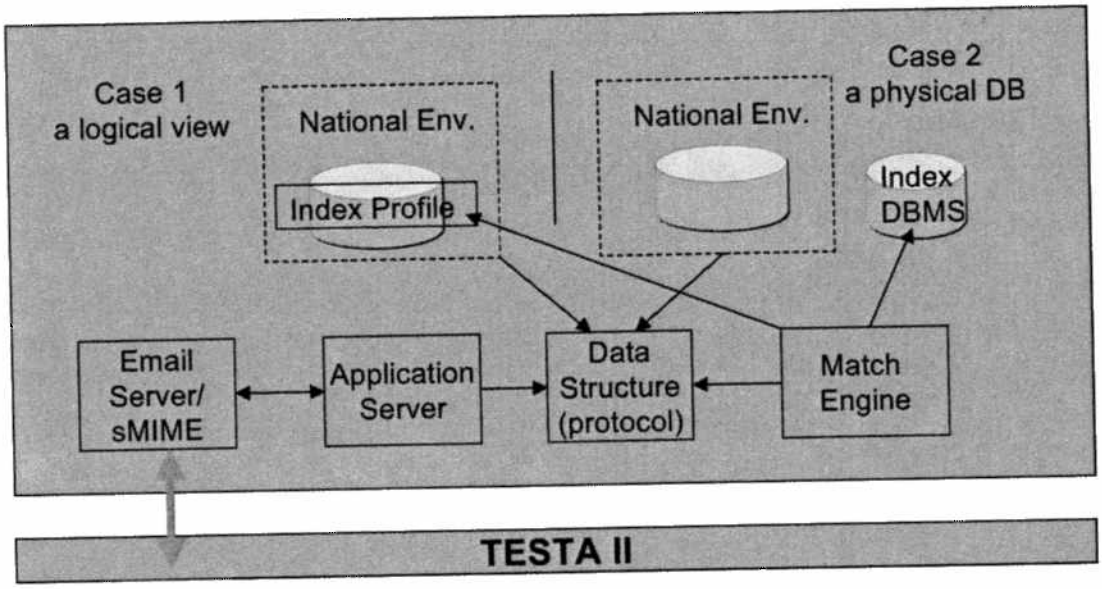
Hver af medlemsstaterne sender de øvrige medlemsstater et sæt standardiserede dna-profiloplysninger, der er i overensstemmelse med det nuværende fælles ICD. Det kan enten ske ved at give en logisk oversigt over den enkelte nationale database eller ved at oprette en fysisk eksporteret database **(indekserede databaser)**.

De fire hovedkomponenter: E-mailserver/S/MIME, Programserver, Datastrukturområde til hentning/fødning af data og registrering af indkommende og udgående meddelelser, og overensstemmelsesmekanismen udmønter hele programmets logik i praksis på en produktuafhængig måde.

For at gøre det lettere for alle medlemsstaterne at integrere komponenterne på deres respektive nationale operationssteder er den specificerede fælles mekanisme blevet indført ved hjælp af open source-komponenter, som de enkelte medlemsstater kan vælge afhængigt af deres nationale it-politik og it-forskrifter. Som følge af de uafhængige faciliteter, der skal indføres for at få adgang til de indekserede databaser, der indeholder de dna-profiler, der er omfattet af afgørelse 2008/.../RIA, kan hver medlemsstat frit vælge sin hardware- og sin softwareplatform, herunder databasesystem og styresystem.

En prototype for udveksling af dna-oplysninger er blevet udviklet og testet med gode resultater via det eksisterende fælles netværk. Version 1.0 er blevet installeret i det aktive miljø og benyttes til de daglige operationer. Medlemsstaterne kan anvende det produkt, der er udarbejdet i fællesskab, men også udvikle deres egne produkter. De fælles produktelementer vil blive vedligeholdt, tilpasset og videreudviklet i takt med it-udviklingen og udviklingen inden for retsmedicin og/eller politiets funktionelle behov.

Fig. 2: Skematisk oversigt over programmet



5.6. Protokoller og standarder, der skal benyttes i programarkitekturen:

5.6.1. XML

Udvekslingen af dna-oplysninger vil fuldt ud udnytte XML-schema som attachment til SMTP e-mail-meddelelser. e**X**tensible **M**arkup **L**anguage (**XML**) er et W3C-anbefalet multifunktionelt opmærkningssprog til udformning af formålsspecifikke opmærkningssprog, som kan beskrive mange forskellige former for data. En dna-profil-beskrivelse, der egner sig til udveksling mellem alle medlemsstaterne, er blevet udarbejdet ved hjælp af XML og XML schema i ICD-dokumentet.

5.6.2. ODBC

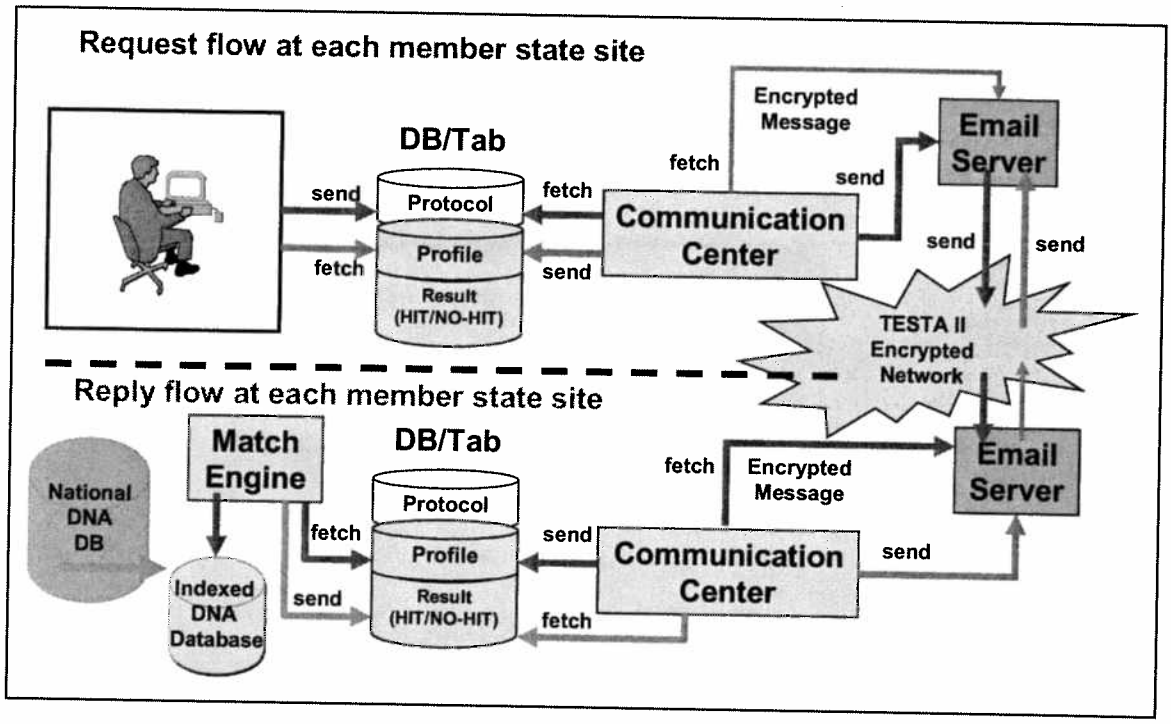
Open **D**ata**B**ase **C**onnectivity giver en standardsoftware API-metode til søgning i databaseforvaltningssystemer og til at gøre søgningen uafhængig af programmeringssprog og af database- og styresystemer. ODBC har imidlertid visse ulemper. Hvis man administrerer et stort antal klientmaskiner, kan der forekomme mange forskellige drivere og DLL-filer. Denne komplekse struktur kan blive en belastning for systemadministrationskapaciteten.

5.6.3. JDBC

Java DataBase Connectivity (JDBC) er et API til Java-programmeringssproget, der definerer, hvordan en klient får adgang til en database. I modsætning til ODBC forudsætter JDBC ikke, at der bruges et bestemt sæt lokale DLL'er på arbejdsstationen.

Arbejdsgangen for behandlingen af anmodninger og svar vedrørende dna-profiler på de enkelte medlemsstaters operationssteder beskrives i nedenstående diagram. Såvel anmodnings- som svarstrømme passerer via et neutralt dataområde, der omfatter forskellige datalagre med en fælles datastruktur.

Fig. 3: Oversigt over arbejdsgangen i databehandlingen på den enkelte medlemsstats operationssted



5.7. Kommunikationsmiljøet

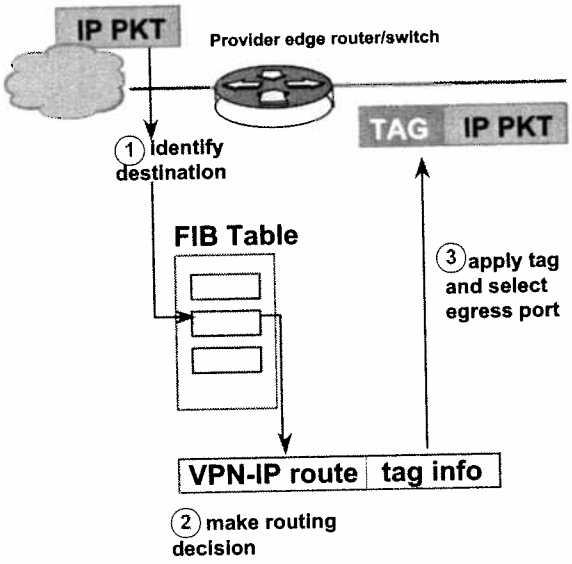
5.7.1. Det fælles kommunikationsnet TESTA og dets opfølgningsinfrastruktur

Programmet til udveksling af dna-oplysninger benytter e-mail, en asynkron mekanisme, til at sende anmodninger og modtage svar medlemsstaterne imellem. Da alle medlemsstaterne har mindst ét nationalt tilkoblingspunkt til TESTA-nettet vil udvekslingen af dna-oplysninger komme til at foregå via TESTA-nettet. TESTA indeholder en række tillægstjenester via sin e-mail relayserver. Foruden at være vært for de specifikke TESTA e-mail-brevkasser gør infrastrukturen det muligt at anvende maildistributionslister og routingpolitikker. Dermed kan TESTA benyttes som clearingorgan for meddelelser, der er stilet til administrationer, som er tilkoblet domænerne for hele EU. Der kan også installeres antivirusmekanismer.

TESTA e-mail relaysystemet er baseret på en high availability hardware platform, der befinder sig på det centrale TESTA programcenter, og som er beskyttet af en firewall. TESTA's **D**omain **N**ame **S**ervices (DNS) står for tildelingen af URL til IP-addresser og skjuler adresseringsoplysninger for brugeren og for programmerne.

5.7.2. Sikkerhedsspørgsmål

Begrebet VPN (Virtual Private Network) er indarbejdet i TESTA. Den Tag Switching Technology, der er benyttet til at opbygge dette VPN, vil blive udviklet til at understøtte en Multi-Protocol Label Switching (MPLS) standard, som er udviklet af Internet Engineering Task Force (IETF).



MPLS er en IETF-standardteknologi, der accelererer nettrafikken ved at undgå at pakkerne analyseres af de mellemliggende routere (hop). Dette sker på grundlag af de såkaldte "labels", som edge-routerne i udkanten af backbonestrukturen knytter til pakken på grundlag af oplysninger, der er lagret i en speciel labeltabel kaldet forwarding information base (FIB). Labels benyttes ligeledes ved oprettelsen af virtual private networks (VPN).

MPLS kombinerer fordelene ved lag 3-routing med fordelene ved lag 2-switching. Eftersom IP-adresserne ikke checkes under transmissionen gennem nettets backbone, sætter MPLS ikke nogen begrænsninger med hensyn til IP-adresserne.

Hertil kommer, at e-mail-meddelelser, der sendes via TESTA, vil være beskyttet af S/MIME's krypteringsmekanisme. Ingen kan uden at kende nøglen og uden at være i besiddelse af det rigtige certifikat dekryptere meddelelser, der sendes via nettet.

5.7.3. Protokoller og standarder, der skal benyttes på kommunikationsnettet

5.7.3.1. SMTP

Simple **M**ail **T**ransfer **P**rotocol er i praksis den gældende standard for e-mail-forsendelse på internettet. SMTP er en forholdsvis enkel tekstbaseret protokol, hvor man angiver en eller flere modtagere af en meddelelse og derefter sender den. SMTP benytter TCP port 25 som specificeret af IETF. Til bestemmelse af SMTP-serveren for et givet domænenavn, benyttes MX (Mail eXchange) DNS (Domain Name Systems) registeret.

Da denne protokol oprindelig udelukkende var baseret på ASCII-tekst, havde den problemer med at klare binære data. Der blev indført standarder som MIME til indkodning af binære data, som skulle transporteres via SMTP. I dag understøtter de fleste SMTP-servere 8BITMIME and S/MIME, der gør det næsten lige så let at sende binære data som almindelig tekst. Reglerne for behandling af S/MIME-operationer er beskrevet i afsnittet om S/MIME (jf. punkt 5.4).

SMTP er en "push"-protokol, der ikke gør det muligt selv at hente ("pull") meddelelser fra en fjernserver. For at kunne gøre dette skal mail-klienten benytte POP3 eller IMAP. Med henblik på udveksling af dna-oplysninger er det blevet besluttet at benytte POP3-protokollen.

5.7.3.2. POP

Lokale e-mail-klienter benytter **P**ost **O**ffice **P**rotocol version **3** (**POP3**), som er en standard-programlagsprotokol til brug på internettet, til at hente e-mail fra en fjernserver via en TCP/IP-forbindelse. Ved at benytte SMTP-protokollens Submit-profil kan e-mail-klienter sende meddelelser via internettet eller via en virksomheds netværk. MIME fungerer som standard for vedhæftede filer og ikke-ASCII-tekst i e-mailen. Selv om hverken POP3 eller SMTP kræver MIME-formateret e-mail, kommer de fleste e-mails på internettet i MIME-format, så POP-klienter er også nødt til at kunne forstå og benytte MIME. Hele kommunikationsmiljøet under afgørelse 2008/.../RIA vil derfor også indeholde POP-komponenterne.

5.7.4. Tildeling af netværksadresser

Det operative miljø

En særskilt klasse C subnetblok er indtil videre blevet tildelt til TESTA af den europæiske IP-registreringsmyndighed (RIPE). TESTA vil efter behov kunne få tildelt yderligere adresseblokke på et senere tidspunkt. IP-adresserne tildeles til medlemsstaterne på grundlag af en geografisk opdeling af Europa. Medlemsstaternes indbyrdes udveksling af oplysninger inden for rammerne af afgørelse 2008/.../RIA, sker via et logisk lukket IP-netværk, der dækker hele Europa.

Testmiljø

Med henblik på at skabe et velfungerende miljø for den daglige drift mellem alle de tilkoblede medlemsstater er det nødvendigt at indrette et testmiljø via det lukkede netværk for nye medlemsstater, der forbereder sig til at komme med i systemet. Der er fastsat et sæt parametre, inkl. IP-adresser, netværksindstillinger, e-mail-domæner samt programbrugerkonti, som skal installeres på den pågældende medlemsstats operationssted. Der er desuden skabt et sæt pseudo-dna-profiler som testen kan køres på.

5.7.5. Konfigureringsparametre

Der er etablere et sikret e-mailsystem på **eu-admin.net**-domænet. Dette domæne og de dertil hørende adresser vil ikke være tilgængelige fra steder, der ikke ligger på TESTA's EU-dækkende domæne, eftersom navnene kun er kendt på TESTA's centrale DNS-server, der er afskærmet fra internettet.

Mappingen af disse TESTA-site-adresser (host names) til deres IP-adresser foretages af TESTA's DNS-tjeneste. For hvert lokalt domæne vil der blive tilføjet en mail-registrering i TESTA's centrale DNS-server, som videresender alle e-mail-meddelelser, der sendes til TESTA's lokale domæner, til TESTA's centrale mail relay server. Herfra sendes de så videre til det specifikke lokale domænes e-mail-server under anvendelse af e-mail-adresser på det lokale domæne. Ved at videresende e-mail på denne måde transporteres de eventuelle kritiske oplysninger i e-mailene kun på den EU-dækkende lukkede netværksinfrastruktur og ikke på det usikre internet.

Der skal oprettes underdomæner (***fede typer og kursiv***) på alle medlemsstaternes operationssteder med følgende syntaks:

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

"Member State-code" antager værdien af en af medlemsstatskoderne med to bogstaver (dvs. AT, BE osv.).

"***application-type***" antager en af følgende to værdier: DNA eller FP.

Efter ovennævnte syntaks kommer medlemsstaternes underdomæner til at se ud som angivet i følgende skema:

MS	Underdomæner	Bemrkninger
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	
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	
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: Udveksling af fingeraftryksoplysninger (Interface Control Document)

Formålet med dette "grænsefladekontroldokument" er at fastsætte, hvilke krav der skal være opfyldt i forbindelse med udveksling af fingertryksoplysninger mellem medlemsstaternes automatiske fingeraftryksidentifikationssystemer (AFIS). Det er baseret på Interpolimplementeringen af ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b).
Denne version skal dække alle de grundlæggende definitioner for logiske records af Type-1, Type-2, Type-4, Type-9, Type-13 og Type-15, som er nødvendige for behandling af fingeraftryk på grundlag af billeder eller minutiae.

1. Oversigt over filens indhold

En fingeraftryksfil består af flere logiske records. I den oprindelige ANSI/NIST-ITL 1-2000 standard var der defineret seksten recordtyper. Der indsættes passende ASCII-adskillelsestegn mellem de enkelte records og felterne og subfelterne inde i de enkelte records.
Til udvekslingen af oplysninger mellem oprindelsesagenturet og modtageragenturet benyttes kun 6 recordtyper:

Type-1 -> Transaction information (Transaktionsoplysninger)
Type-2 -> Alphanumeric persons/case data (Alfanumeriske data om personer eller sager)
Type-4 -> High resolution grayscale dactyloscopic images (Gråtonebilleder med høj opløsning af fingeraftryk)
Type-9 -> Minutiæ Record (Minutiae)
Type-13 -> Variable resolution latent image record (Latent billede med variabel opløsning)
Type-15 -> Variable resolution palmprint image record (Håndfladeaftryksbillede med variabel opløsning)

1.1. Type-1 - File header

Denne record indeholder routingoplysninger og oplysninger, der beskriver resten af filens struktur. Denne recordtype definerer også de typer af transaktioner, der henhører under følgende brede kategorier:

1.2. Type-2 - Descriptive text

Denne record indeholder tekstoplysninger af interesse for de afsendende og modtagende agenturer.

1.3. Type-4 - High resolution gray-scale image

Denne record benyttes til udveksling af gråtonebilleder (otte bit) af fingeraftryk med høj opløsning (500 DPI). Fingeraftryksbillederne komprimeres efter WSQ-algoritmen i et forhold på højst 15:1. Andre komprimeringsalgoritmer eller ukomprimerede billeder må ikke benyttes.

1.4. Type-9 - Minutiae record

Type-9 records benyttes til udveksling af linjekarakteristika eller minutiae-data. Formålet er dels at undgå unødig dobbelt udførelse af AFIS-indkodningen og dels at gøre det muligt at sende AFIS-koderne, der indeholder færre data end de tilsvarende billeder.

1.5. Type-13 - Variable-Resolution Latent Image Record

Denne record benyttes til udveksling af latente fingeraftryksbilleder og latente håndfladeaftryksbilleder med variabel opløsning ledsaget af alfanumeriske teksturoplysninger. Billederne skannes med en opløsning på 500 DPI med 256 gråtoner. Hvis det latente billedes kvalitet er tilstrækkelig god, komprimeres det efter WSQ-algoritmen. Om nødvendigt kan billedopløsningen øges til mere end 500 DPI og mere end 256 gråtoner efter aftale mellem to parter. I så tilfælde anbefales det kraftigt at benytte JPEG 2000 (jf. Tillæg 7).

1.6. Variable-Resolution Palmprint Image Record

Type-15-billed-records med mærkede felter benyttes til udveksling af håndfladeaftryksbilleder med variabel opløsning sammen med alfanumeriske teksturoplysninger. Billederne skannes med en opløsning på 500 DPI og med 256 gråtoner. For at begrænse datamængden bør alle håndfladeaftryksbilleder komprimeres efter WSQ-algoritmen. Om nødvendigt kan billedopløsningen øges til mere end 500 DPI og mere end 256 gråtoner efter aftale mellem to parter. I så tilfælde anbefales det kraftigt at benytte JPEG 2000 (jf. Tillæg 7).

2. Record-formatet

En transaktionsfil består af en eller flere logiske records. For hver logisk record, som filen indeholder, skal der være en række informationsfelter, der passer til den pågældende recordtype. Hvert af informationsfelterne kan indeholde et eller flere grundlæggende informationselementer, der hver især består af en enkelt værdi. Tilsammen benyttes disse elementer til at angive forskellige aspekter af oplysningerne i feltet. Et informationsfelt kan også bestå af et eller flere informationselementer, der grupperes og gentages flere gange i et felt. En sådan gruppe af informationselementer kaldes et subfelt. Et informationsfelt kan således bestå af et eller flere subfelter med informationselementer.

2.1. Information separators

I de logiske records med mærkede felter er der indsat mekanismer til adskillelse af oplysningerne, som benytter fire ASCII-informationsseparatorer. De adskilte oplysninger kan være elementer i et felt eller subfelt, felter inden for en logisk record eller subfelter, der forekommer flere gange. De benyttede informationsseparatorer er defineret i standarden ANSI X3.4. Disse tegn benyttes til at adskille og karakterisere information på en logisk måde. Set ud fra en hierarkisk synsvinkel er filseparatortegnet "FS" det mest inklusive, og derefter følger gruppeseparatortegnet "GS", recordseparatortegnet "RS og endelig enhedsseparatortegnet "US". Tabel 1 viser disse ASCII-separatorer og giver en beskrivelse af deres brug i forbindelse med denne standard.

Informationsseparatorer bør funktionelt set betragtes som en angivelse af, hvilken type data der følger efter. "US"-tegnet adskiller individuelle informationselementer inde i et felt eller subfelt. Dette signalerer, at det efterfølgende informationselement vedrører det pågældende felt eller subfelt. En række subfelter i et felt, som er adskilt af "RS"-tegnet, angiver starten af den næste gruppe af gentagne informationselementer. "GS"-separatortegnet, der benyttes mellem informationsfelter, angiver starten af et nyt felt, der efterfølges af det angivne feltidentificeringsnummer. På tilsvarende vis markeres begyndelsen af en ny logisk record med angivelse af tegnet "FS".

De fire tegn giver kun mening, når de benyttes som separatorer mellem dataelementer i felter i ASCII-tekstrecords. Tegnene har ingen specifik betydning, når de forekommer i binære billedrecords og binære felter - de indgår blot som en del af de udvekslede oplysninger.

Normalt bør der ikke være nogen tomme felter eller informationselementer, så der bør derfor kun være ét separatortegn mellem to givne dataelementer. Undtagelsen fra denne regel indtræder, når data i felterne eller informationselementer i en transaktion ikke er tilgængelige, ikke findes eller er fakultative, og behandlingen af transaktionen ikke er afhængig af, at de pågældende data er til stede. I sådanne tilfælde skal man angive flere separatortegn i træk snarere end at indsætte fylddata mellem separatortegnene.

Med henblik på definitionen af et felt, der består af tre informationselementer, gælder følgende.

Hvis oplysningerne i det andet informationselement mangler, anføres der to "US" informationsseparatortegn ved siden af hinanden mellem det første og det tredje informationselement. Hvis både andet og tredje informationselement mangler, anføres der tre separatortegn - to "US"-tegn samt det afsluttende separatortegn for feltet eller subfeltet. Som hovedregel bør det korrekte antal separatortegn indsættes, hvis et eller flere obligatoriske eller fakultative informationselementer ikke er tilgængelige for et felt eller subfelt.

Det er muligt at have kombinationer af to eller flere af de fire separatortegn lige efter hinanden. Hvis dataene ikke foreligger eller ikke er tilgængelige til informationselementer, subfelter eller felter, skal der være et separatortegn mindre end det fornødne antal informationselementer, subfelter eller felter.

Table 1: Benyttede separatorer

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

2.2. Record layout

I logiske records med mærkede felter, skal hvert af de benyttede informationsfelter nummereres i overensstemmelse med denne standard. Formatet for hvert felt skal bestå af den logiske records typenummer efterfulgt af et punktum ".", et feltnummer efterfulgt af et kolon ":", efterfulgt af de oplysninger, der skal stå i feltet. Det mærkede felts nummer er et etcifret tal fra 1 til 9, som anføres mellem punktummet "." og kolonet ":". Det skal fortolkes som et nummer i et usigneret talfelt. Det vil sige, at feltnummeret "2.123:" svarer til og skal fortolkes på samme måde som feltnummeret "2.000000123:".

I eksemplerne i resten af dette dokument benyttes et trecifret tal til angivelse af felterne i hver af de logiske records med mærkede felter, der beskrives heri. Feltnumrene udformes således: "TT.xxx:", hvor "TT" repræsenterer recordtypen med et eller to tegn efterfulgt af et punktum. De næste tre tegn angiver det pågældende feltnummer efterfulgt af et kolon. Efter kolonet følger der beskrivende ASCII-oplysninger eller billeddata.

Logiske records af Type 1 og Type 2 indeholder kun ASCII tekstdatafelter. Recordens samlede længde (inkl. feltnumre, koloner og separatortegn) skal angives som det første ASCII-felt i hver af disse recordtyper. ASCII-filseparatorkontroltegnet "FS" (der angiver afslutningen af den logiske record eller transaktion) skal følge umiddelbart efter sidste byte i ASCII-oplysningerne og skal medregnes i recordens længde.

Modsat hvad der gælder for mærkede felter, indeholder en Type-4 record kun binære data, der er registreret som ordnede binære felter med fast længde. Recordens samlede længde skal angives i det første binære fire-byte-felt i hver record. Hverken recordnummeret med efterfølgende punktum eller feltidentifikationsnummeret med efterfølgende kolon skal registreres for denne binære record. Hertil kommer, at da alle felterne i denne record enten har fast eller specificeret længde, skal ingen af de fire separatortegn ("US", "RS", "GS", eller "FS") fortolkes som andet end binære data. I den binære record skal tegnet "FS" ikke benyttes som recordseparator eller som transaktionsafslutningstegn.

3. Type-1 logisk record: filens header

Denne record beskriver filens struktur og type og andre vigtige oplysninger. Det tegnsæt, der anvendes i type 1-felter, må kun indeholde 7-bit-ANSI-koden for udveksling af oplysninger.

3.1. Fields for Type-1 Logical Record

3.1.1. Felt 1.001: Den logiske records længde (LEN)

Dette felt angiver det samlede antal bytes i hele den logiske record af Type-1. Feltet begynder med "1.001:" efterfulgt af recordens samlede længde, hvori medtages samtlige tegn i hvert eneste felt og informationsseparatorerne.

3.1.2. Field 1.002: Version Number (VER)

For at sikre, at brugerne er opmærksomme på, hvilken version af ANSI/NIST-standarden, der benyttes, angiver dette fire-byte-felt nummeret på den version af standarden, der benyttes af softwaren eller af det system, der har genereret filen. De første to bytes specificerer hovedversionens referencenummer og de næste to nummeret på det sekundære revisionsnummer. Eksempelvis anses den oprindelige 1986-standard for at være den første version, der angives som "0100", medens den nuværende ANSI/NIST-ITL 1-2000 standard angives som "0300".

3.1.3. Field 1.003: File Content (CNT)

Dette felt angiver hver eneste record i filen efter recordtype og den rækkefølge, som disse records optræder i i den logiske fil. Det består af et eller flere subfelter, der hvert især indeholder to informationselementer, der beskriver en enkelt logisk record, der forekommer i den pågældende fil. Subfelterne angives i den rækkefølge, som de pågældende records er registreret og sendt i.

Det første informationselement i det første subfelt er "1", som henviser til denne Type-1 record. Det efterfølges af et andet informationselement, der angiver, hvor mange andre records filen indeholder. Dette nummer er også lig med antallet af resterende subfelter under felt 1.003.

Hvert af de øvrige subfelter associeres med en record i filen, og subfeltsekvensen svarer til recordsekvensen. Hvert subfelt indeholder to informationselementer. Det første identificerer recordtypen. Det andet er recordens IDC. "*US*"-tegnet benyttes til at adskille de to informationselementer.

3.1.4. Field 1.004: Type of Transaction (TOT)

Dette felt indeholder et mnemoteknisk hjælpemiddel på tre bogstaver, som angiver transaktionstypen. Disse koder kan være forskellige fra dem, der benyttes af andre implementeringer af ANSI/NIST-standarden.

CPS: Criminal Print-to-Print Search. Denne transaktion er en anmodning om en søgning i en aftryksdatabase på en record vedrørende en lovovertrædelse. Personens aftryk skal medsendes som WSQ-komprimerede billeder i filen.

I tilfælde af **No-HIT** (ingen overensstemmelse), vil følgende logiske records blive sendt tilbage:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

I tilfælde af **HIT** (overensstemmelse), vil følgende logiske records blive sendt tilbage:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

⇒ 1-14 Type-4 Record

CPS TOT er sammenfattet i **Tabel A.6.1** (Tillæg 6).

PMS: Print-to-Latent Search. Denne transaktion benyttes, når der skal søges efter overensstemmelse med et sæt aftryk i en database over uidentificerede latente aftryk. Svaret vil indeholde **Hit/No-Hit**-afgørelsen af destinationens søgning i fingeraftryksidentifikationssystemet. Hvis der forekommer flere uidentificerede latente aftryk, vil der blive tilbagesendt flere SRE-transaktioner med et latent aftryk pr. transaktion. Personens aftryk skal medsendes som WSQ-komprimerede billeder i filen.

I tilfælde af **No-HIT** (ingen overensstemmelse), vil følgende logiske records blive sendt tilbage:
⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

I tilfælde af **HIT**(overensstemmelse), vil følgende logiske records blive sendt tilbage:
⇒ 1 Type-1 Record
⇒ 1 Type-2 Record
⇒ 1 Type-13 Record
PMS TOT er sammenfattet i **Tabel A.6.1** (Tillæg 6).

MPS: Latent-to-Print Search. Denne transaktion benyttes, når der skal søges efter overensstemmelse med et latent aftryk i en fingeraftryksdatabase. Minutiae om det latente aftryk og billedet (WSQ-komprimeret) skal medsendes i filen.

I tilfælde af **No-HIT** (ingen overensstemmelse), vil følgende logiske records blive sendt tilbage:
⇒ 1 Type-1 Record
⇒ 1 Type-2 Record

I tilfælde af **HIT**(overensstemmelse), vil følgende logiske records blive sendt tilbage:
⇒ 1 Type-1 Record
⇒ 1 Type-2 Record
⇒ 1 Type-4 or Type-15 Record
MPS TOT er sammenfattet i **Tabel A.6.4** (Tillæg 6).

MMS: Latent-to-Latent Search. I denne transaktion indeholder filen et latent aftryk, som der skal søges på i en database over uidentificerede latente aftryk for at etablere forbindelser mellem forskellige gerningssteder. De detaljerede oplysninger om det latente aftryk og billedet (WSQ-komprimeret) skal medsendes i filen.

I tilfælde af **No-HIT** (ingen overensstemmelse), vil følgende logiske records blive sendt tilbage:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

I tilfælde af **HIT** (overensstemmelse), vil følgende logiske records blive sendt tilbage:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

⇒ 1 Type-13 Record

MMS TOT er sammenfattet i **Tabel A.6.4** (Tillæg 6).

SRE: Denne transaktion sendes tilbage af det anmodede agentur som svar på fingeraftryksforespørgsler. Svaret vil indeholde **Hit/No-Hit**-afgørelsen af destinationens søgning i fingeraftryksidentifikationssystemet. Hvis der forekommer flere kandidater, vil der blive tilbagesendt flere SRE-transaktioner med én kandidat pr. transaktion.

SRE TOT er sammenfattet i **Tabel A.6.2** (Tillæg 6).

ERR: Denne transaktion sendes tilbage af det anmodede fingeraftryksidentifikationssystem for at angive en fejl i forbindelse med transaktionen. Den indeholder et meddelelsesfelt (**ERM**), der angiver, hvilken fejl der er konstateret. Følgende logiske records vil blive sendt tilbage:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

ERR TOT er sammenfattet i **Tabel A.6.3** (Tillæg 6).

Table 2: Tilladte koder i transaktionerne

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

Key:

M = Mandatory (obligatorisk)

M* = Kun én af de to recordtyper kan medtages

O = Optional (fakultativ)

C = Conditional (afhængigt af, om oplysningerne er tilgængelige)

- = Ikke tilladt

1* = Afhængigt af legacy-systemerne

3.1.5. Field 1.005: Date of Transaction (DAT)

Dette felt angiver den dato, hvor transaktionen blev indledt, og skal følge ISO-standardformatet være: YYYYMMDD

hvor YYYY er året, MM er måneden, og DD er dagen. Der sættes et nul foran étcifrede tal. For eksempel svarer "19931004" til den 4. oktober 1993.

3.1.6. Field 1.006: Priority (PRY)

Dette fakultative felt definerer den prioritet, på en skala fra 1 til 9, som tillægges søgningen. "1" er højeste prioritet og "9" laveste prioritet. Transaktioner med prioritet "1" skal behandles omgående.

3.1.7. Field 1.007: Destination Agency Identifier (DAI)

Dette felt angiver det agentur, som transaktionen er rettet til.

Det består af to informationselementer i følgende format: CC/*agency*.

Det første informationselement indeholder landekoden (Country Code), som er defineret i ISO 3166, og som består af to alfanumeriske tegn. Det andet element, *agenturet (agency)*, er en fritekstidentificering af agenturet på højst 32 alfanumeriske tegn.

3.1.8. Field 1.008: Originating Agency Identifier (ORI)

Dette felt angiver det agentur, der har afsendt filen, og det er i samme format som DAI (Felt 1.007).

3.1.9. Field 1.009: Transaction Control Number (TCN)

Dette er et kontrolnummer til henvisningsbrug. Det genereres af computeren og har følgende format: YYSSSSSSSSA

hvor YY er transaktionsåret, SSSSSSSS er et ottecifret serienummer og A er et kontrolbogstav, der genereres efter proceduren i Tillæg 2.

Når TCN ikke er til rådighed, udfyldes feltet YYSSSSSSSS, med nuller, og kontrolbogstavet genereres som angivet ovenfor.

3.1.10. Field 1.010: Transaction Control Response (TCR)

Når en søgning er sendt afsted, og dette svar kommer tilbage, vil dette fakultative felt indeholde søgningsmeddelelsens transaktionskontrolnummer. Det har derfor samme format som TCN (Felt 1.009).

3.1.11. Field 1.011: Native Scanning Resolution (NSR)

Dette felt angiver den normale scanningsopløsning i det system, som transaktionsafsenderen understøtter. Opløsningen angives som et tocifret tal, efterfulgt af et decimalkomma og derefter endnu to cifre.

For alle transaktioner i henhold til afgørelse 2008/.../RIA skal opløsningen være på 500 DPI (=pixels/inch) eller 19,68 pixels/mm.

3.1.12. Field 1.012: Nominal Transmitting Resolution (NTR)

Dette felt på fem byte angiver den nominelle overførselsopløsning for de billeder, der overføres. Opløsningen angives i pixels/mm i samme format som NSR (Felt 1.011).

3.1.13. Field 1.013: Domain name (DOM)

Dette obligatoriske felt angiver domænenavnet for implementeringen af den brugerdefinerede logiske type-2-record. Det består af to informationselementer og skrives således: "INT-I{US}4.22{GS}".

3.1.14. Field 1.014: Greenwich mean time (GMT)

Dette obligatoriske felt tilvejebringer en mekanisme til at udtrykke dato og klokkeslæt udtrykt i universelle Greenwich Mean Time (GMT) enheder. Når det benyttes, indeholder GMT-feltet den universelle dato, som supplerer den lokale dato i felt 1.005 (DAT). Brugen af GMT-feltet fjerner det problem med lokal tid, der opstår, når en transaktion og svaret herpå sendes mellem to steder, der er adskilt af flere tidszoner. GMT angiver den universelle dato og klokkeslæt døgnet rundt uafhængig af tidszoner. Den angives som "CCYYMMDDHHMMSSZ", en sekvens på 15 tegn, der kæder datoen sammen med GMT og slutter med et "Z". Tegnene "CCYY" angiver transaktionsåret, "MM" angiver måneden med to cifre, og "DD" angiver dagen med to cifre, "HH" står for timetallet, "MM" for minuttallet og "SS" for sekundtallet. Den fulde dato må ikke være senere end dags dato.

4. Type-2 Logisk record: beskrivende tekst

Strukturen i det meste af denne record er ikke defineret efter den oprindelige ANSI/NIST-standard. Den indeholder oplysninger af specifik interesse for de agenturer, der afsender eller modtager filen. For at sikre kompatibiliteten mellem fingeraftrykssystemer, der skal kommunikere med hinanden, er det nødvendigt, at recorden kun indeholder de felter, der er angivet nedenfor. Dette dokument angiver, hvilke felter der er obligatoriske, og hvilke der er fakultative, og definerer desuden de enkelte felters struktur.

4.1. Felter i logisk record af Type-2

4.1.1. Field 2.001: Logical Record Length (LEN)

Dette felt angiver den samlede længde af hele den logiske record af Type-2 og angiver det samlede antal bytes, inkl. samtlige tegn i hvert enkelt felt og informationsseparatorerne.

4.1.2. Field 2.002: Image Designation Character (IDC)

Den IDC, der anføres i dette obligatoriske felt, er en ASCII-representation af IDC som defineret i filindholdsfeltet (CNT) for records af Type-1 (felt 1.003).

4.1.3. Field 2.003: System Information (SYS)

Dette felt er obligatorisk og indeholder fire bytes, der angiver, hvilken version af INT-I denne specifikke Type-2 record er forenelig med.

De første to bytes specificerer hovedversionens referencenummer og de næste to nummeret på det sekundære revisionsnummer. Eksempelvis er denne implementering baseret på INT-I version 4 revision 22 og skal derfor angives som "0422".

4.1.4. Field 2.007: Case Number (CNO)

Dette nummer tildeles af det lokale fingeraftrykskontor til en række latente aftryk, der er fundet på et gerningssted. Det angives i følgende format: CC/*number*

hvor CC er Interpols landekode på to alfanumeriske tegn, og "*number*" afhænger af de relevante lokale retningslinjer og kan være op til 32 alfanumeriske tegn lang.

Dette felt gør det muligt for systemet at identificere latente aftryk med tilknytning til en bestemt lovovertrædelse.

4.1.5. Field 2.008: Sequence Number (SQN)

Dette felt angiver hver sekvens af latente aftryk i en sag. Det kan være op til fire numeriske tegn langt. En sekvens er et latent aftryk eller en række latente aftryk, der er grupperet med henblik på lagring og/eller søgning. Definitionen indebærer, at selv individuelle latente aftryk også skal have tildelt et sekvensnummer.

Dette felt kan sammen med MID (felt 2.009) medtages med henblik på at identificere et bestemt latent aftryk i en sekvens.

4.1.6. Field 2.009: Latent Identifier (MID)

Dette felt angiver det enkelte latente aftryk i en sekvens. Værdien er et eller to bogstaver, hvor "A" betegner det første latente aftryk, "B" det andet og så videre op til "ZZ". Dette felt benyttes på samme måde som det latente sekvensnummer, der er omhandlet i beskrivelsen af SQN (felt 2.008).

4.1.7. Field 2.010: Criminal Reference Number (CRN)

Dette er et unikt referencenummer, som et nationalt agentur tildeler til en person, der for første gang tiltales for en lovovertrædelse. I det enkelte land har den enkelte aldrig mere end ét CRN og har det heller ikke til fælles med nogen anden person. Men den samme person kan have strafferetlige referencenumre i flere lande, som skelnes fra hinanden ved hjælp af landekoderne.

Følgende format benyttes for CRN-feltet: CC/*number*

hvor CC er den landekode på to alfanumeriske tegn, som er defineret i ISO 3166, og *number* afhænger af det udstedende agenturs relevante lokale retningslinjer og kan være op til 32 alfanumeriske tegn lang.

For transaktioner i henhold til afgørelse 2008/.../RIA vil dette felt blive benyttet til det anmodende agenturs nationale strafferetlige referencenummer, som er knyttet til billederne i records af type 4 eller type 15.

4.1.8. Field 2.012: Miscellaneous Identification Number (MN1)

Dette felt indeholder CRN (felt 2.010), som er overført ved en CPS- eller PMS-transaktion uden landekode foran.

4.1.9. Field 2.013: Miscellaneous Identification Number (MN2)

Dette felt indeholder CNO (felt 2.007), som er overført ved en MPS- eller MMS-transaktion uden landekode foran.

4.1.10. Field 2.014: Miscellaneous Identification Number (MN3)

Dette felt indeholder SQN (felt 2.008), som er overført ved en MPS- eller MMS-transaktion.

4.1.11. Field 2.015: Miscellaneous Identification Number (MN4)

Dette felt indeholder MID (felt 2.009), som er overført ved en MPS- eller MMS-transaktion.

4.1.12. Field 2.063: Additional information (INF)

I tilfælde af en SRE-transaktion i forbindelse med en PMS-anmodning indeholder dette felt oplysninger om, hvilken finger, der gav den eventuelle overensstemmelse. Feltets format er som følger:

NN *hvor NN* er den fingerpositionskode, der er defineret i tabel 5, på to tegns længde.

I alle andre tilfælde er feltet fakultativt. Det består af op til 32 alfanumeriske tegn og kan give supplerende information om anmodningen.

4.1.13. Field 2.064: Respondents List (RLS)

Dette felt indeholder mindst to subfelter. Det første subfelt beskriver, hvilken type søgning der er foretaget, ved hjælp af et mnemoteknisk hjælpemiddel på tre bogstaver, som angiver transaktionstypen i TOT (felt 1.004). Det andet subfelt er kun på ét tegn. Et "**I**" angiver, at der er fundet en overensstemmelse (HIT), og "**N**" angiver, at der ikke er fundet nogen overensstemmelse (NOHIT). Det tredje subfelt indeholder sekvensidentifikatoren for kandidatresultatet og det samlede antal kandidater, adskilt af en skråstreg. Hvis der findes flere kandidater, vil der blive sendt flere meddelelser tilbage.

I tilfælde af en mulig overensstemmelse vil det fjerde subfelt indeholde resultatet i form af et tal med op til seks cifre. Er overensstemmelsen bekræftet, angives værdien i subfeltet til "999999".

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

Hvis AFIS-fjernserveren ikke sætter tal på resultatet, bør resultatet nul benyttes på det pågældende punkt.

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

Dette felt indeholder fejlmeddelelser i tilknytning til transaktioner, som vil blive sendt tilbage til anmoderen, når der opstår en fejl.

Tabel 3: Fejlmeddelelser

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.

Fejlmeddelelse 100-199:

Disse fejlmeddelelser vedrører valideringen af ANSI/NIST-records og defineres som:

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

<error_code 2>: IDC <idc_number 2> FIELD <field_id 2> <dynamic text 2>…

hvor

error_code er en kode, der entydigt angiver en specifik årsag (jf. tabel 3)

- field_id er ANSI/NIST-feltnummeret for det felt, som fejlen vedrører (e.g. 1.001, 2.001, ...) i formatet <record_type>.<field_id>.<sub_field_id>
- dynamisk tekst er en mere detaljeret dynamisk beskrivelse af fejlen
- LF betegner et linjeskift (Line Feed), der adskiller fejlene, hvis der konstateres mere end én fejl
- for type-1 records er ICD defineret som "-1"

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

Dette felt er obligatorisk for fejltransaktioner.

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

Dette felt indeholder det maksimale antal kandidater, som det anmodende agentur forventer at skulle kontrollere. ENC-værdien må ikke overstige de værdier, der er fastsat i tabel 11.

5. Type-4 logisk record: Gråtonebillede med høj opløsning

Det skal bemærkes, at type-4 records i sagens natur er binære og ikke ASCII-baserede. Derfor har hvert enkelt felt fået anvist en bestemt position i recorden, hvilket indebærer, at alle felterne er obligatoriske.

Standarden gør det muligt at angive såvel billedets størrelse som opløsningen i recorden. Kun logiske records af type 4 kan indeholde fingeraftryksbilleddata, der overføres med en nominel pixeltæthed på 500-520 DPI. Den foretrukne pixeltæthed for nye miljøer er 500 DPI (pixels/inch) eller 19,68 pixels/mm. 500 DPI er den tæthed, der anbefales af INT-I, men tilsvarende systemer kan kommunikere med hinanden ved en anden tæthed end den foretrukne, beliggende mellem 500 og 520 DPI.

5.1. Felter i logiske records af type 4

5.1.1. Field 4.001: Logical Record Length (LEN)

Dette felt på fire bytes angiver længden af denne type-4-record og angiver det samlede antal bytes, inkl. samtlige bytes i hvert enkelt felt i recorden.

5.1.2. Field 4.002: Image Designation Character (IDC)

Dette er den 1 byte store binære repræsentation af det IDC-nummer, der er angivet i headerfilen.

5.1.3. Field 4.003: Impression Type (IMP)

Aftrykstypen er et 1 byte stort felt, der optræder som den sjette byte i recorden.

Tabel 4 : Fingeraftrykstype

Code	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper
4	Latent impression captured directly
5	Latent tracing
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4 Field 4.004: Finger Position (FGP)

Dette felt, der har en fast længde på 6 bytes, optræder som bytes nr. 7-12 i en type-4 record. Det angiver mulige fingerpositioner begyndende i den byte, der er længst til venstre (byte 7 i recorden). Den kendte eller mest sandsynlige fingerposition hentes i tabel 5. Der kan registreres yderligere fem fingre ved at indlæse de øvrige fingerpositioner i de resterende fem bytes efter samme model. Hvis der benyttes færre end fem registrerede fingerpositioner, udfyldes de ubenyttede bytes med det binære 255. Til registrering af alle fingerpositionerne benyttes koden 0 for ukendt.

Tabel 5: Fingerpositionskode og maksimal størrelse

Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40.0	40.0
Right thumb	1	45.0	40.0
Right index finger	2	40.0	40.0
Right middle finger	3	40.0	40.0
Right ring finger	4	40.0	40.0
Right little finger	5	33.0	40.0
Left thumb	6	45.0	40.0
Left index finger	7	40.0	40.0
Left middle finger	8	40.0	40.0
Left ring finger	9	40.0	40.0
Left little finger	10	33.0	40.0
Plain right thumb	11	30.0	55.0
Plain left thumb	12	30.0	55.0
Plain right four fingers	13	70.0	65.0
Plain left four fingers	14	70.0	65.0

For latente aftryk fra gerningssteder benytter man kun koderne 0 til 10.

5.1.5. Field 4.005: Image Scanning Resolution (ISR)

Dette 1 byte store felt optræder som byte nr. 13 i en type-4 record. Hvis værdien er "0" er billedet taget med den foretrukne scanningsopløsning på 19,68 pixels/mm (500 pixels/inch). Hvis værdien er "1", er billedet optaget med en anden scanningsopløsning, som angivet i type 1-recorden.

5.1.6. Field 4.006: Horizontal Line Length (HLL)

Dette felt optræder som byte nr. 14 og 15 i en type-4 record. Det angiver antallet af pixels i hver scannet linje. Den første byte er den vigtigste.

5.1.7. Field 4.007: Vertical Line Length (VLL)

Dette felt angiver i byte nr. 16 og 17 antallet af scannede linjer i billedet. Den første byte er den vigtigste.

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

Dette 1 byte store felt angiver, hvilken gråtonekomprimeringsalgoritme, der er benyttet ved kodningen af billeddataene. I denne implementering angiver en binær kode 1, at WSQ-komprimeringsalgoritmen (Tillæg 7) er benyttet.

5.1.9. Field 4.009: The Image

Dette felt indeholder en byte-strøm, der repræsenterer billedet. Strukturen vil naturligvis afhænge af den benyttede komprimeringsalgoritme.

6. Type-9 logisk record: Minutiae Record

Type-9-records indeholder ASCII-tekst, der beskriver minutiæ og dertil knyttede oplysninger, som er indkodet fra et latent aftryk. For en søgetransaktion på et latent aftryk er der ingen begrænsning for, hvor mange af disse type-9-records, en fil kan indeholde, og som hver især skal svare til et særskilt view eller latent aftryk.

6.1. Minutiae extraction

6.1.1. Minutia type identification

Denne standard definerer tre identifikationsnumre, der benyttes til at beskrive, hvilken type minutia der er tale om. De er anført i tabel 6. En linjeafslutning (ridge ending) betegnes som type 1. En bifurcation betegnes som type 2. Hvis en minutia ikke klart kan kategoriseres som en af disse typer, betegnes den som "andet", type 0.

Table 6: Minutia types

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

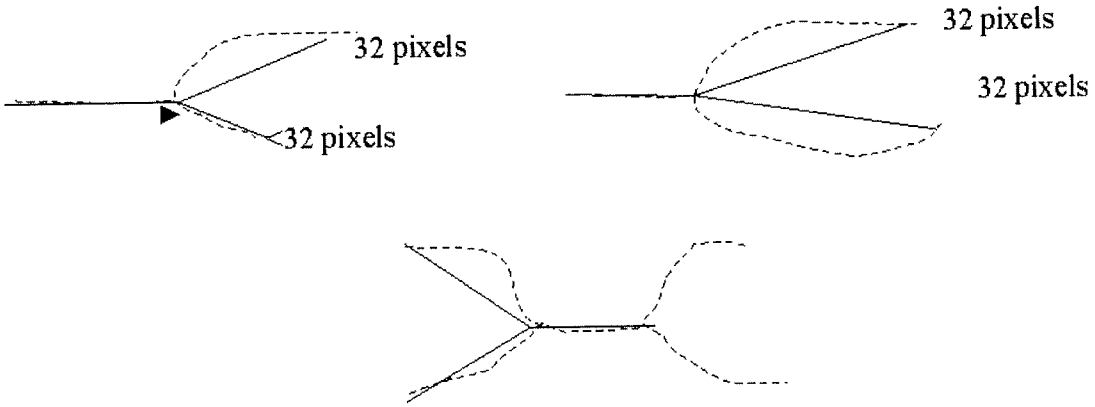
6.1.2. Minutia placement and type

For at modellerne kan være i overensstemmelse med afsnit 5 i ANSI INCITS 378-2004-standarden, skal følgende metode, der er en udbygning af den nuværende INCITS 378-2004-standard, benyttes til at bestemme de enkelte minutiaes position (lokalisering og retning).

Den position eller lokalisering, som en minutia, der repræsenterer en linjeafslutning, har, bliver forgreningspunktet for midterskelettet i fordybningen foran linjeforhøjningens afslutning. Hvis man reducerer de tre udløbere i fordybningen til et skelet af kun én pixels bredde, vil krydspunktet være minutia'ens lokalisering. Tilsvarende er en bifurcations lokalisering forgreningspunktet for linjeforhøjningens midterskelet. Hvis forhøjningens tre udløbere hver især blev reduceret til et skelet af kun én pixels bredde, ville de tre udløberes krydspunkt være minutia'ens lokalisering.
Når alle linjeafslutningerne er blevet konverteret til bifurcationer, repræsenteres alle fingeraftrykkets minutiae som bifurcationer. X- og Y-pixelkoordinaterne i krydspunktet for de tre udløbere af hver minutia kan formateres direkte. Fastsættelsen af minutiaernes retning kan udledes af hver af skelettets bifurcationer. De tre udløbere af hvert af skelettets bifurcationer skal undersøges, og endepunktet for hver udløber lokaliseres. Figur 6.1.2 illustrerer de tre metoder, der benyttes til at lokalisere endepunktet for en udløber på grundlag af en scanningsopløsning på 500 DPI.
Endepunktet lokaliseres ud fra den begivenhed, der indtræder først. Pixeltællingen er baseret på en scanningsopløsning på 500 DPI. Men andre scanningsopløsninger vil pixeltællingen give andre resultater.

- En afstand på 0,064" (den 32. pixel)
- Endepunktet for skeletudløberen befinder sig i en afstand af mellem 0,02" og 0,064" (fra den 10. til den 32. pixel); kortere udløbere benyttes ikke
- En anden bifurcation optræder inden for en afstand af 0,064" (før den 32. pixel)

Figur 6.1.2



Minutiaevinklen bestemmes ved at konstruere tre virtuelle stråler, der starter ved bifurcationspunktet og når ud til enden af hver udløber. Medianlinjen i den mindste af de tre vinkler, som disse stråler danner, angiver minutiaens retning.

6.1.3. Koordinatsystem

Det koordinatsystem, der benyttes til at anskueliggøre et fingeraftryks minutiae, er et kartesisk koordinatsystem. Lokaliseringen af de enkelte minutiae repræsenteres af deres x- og y-koordinater. Koordinatsystemets origo placeres i det oprindelige billedes øverste venstre hjørne, således at x-værdierne stiger mod højre og y-værdierne stiger i nedadgående retning. Både x- og y-koordinaterne for et minutia angives i pixelenheder fra origo. Det skal bemærkes, at placeringen af origo og måleenhederne ikke er i overensstemmelse med den konvention, der anvendes i definitionerne af type 9 i ANSI/NIST-ITL I-2000.

6.1.4. Minutiaeernes retning

Vinklerne udtrykkes i matematisk standardformat, med 0 grader til højre og vinkler, der bliver større mod uret. De registrerede vinkler åbner bagud langs forhøjningen for en forhøjningsafslutning og i retning mod fordybningens midte for en bifurcation. Denne konvention er 180° modsat den konventionelle vinkel, der beskrives i definitionerne af type 9 i ANSI/NIST-ITL I-2000.

6.2. Felter i type-9 logisk record INCITS-378 format

Alle felter i type-9 recorden registreres som ASCII tekst. Der må ikke være nogen binære felter i denne record med mærkede felter.

6.2.1. Field 9.001: Logical record length (LEN)

Dette obligatoriske ASCII felt skal angive længden af den logiske record og præcisere det samlede antal bytes, herunder hvert tegn i hvert felt i recorden.

6.2.2. Field 9.002: Image designation character (IDC)

Dette obligatoriske to-byte felt anvendes til identificering og placering af minutiaedata. IDC i dette felt skal matche IDC i feltet for filindhold i type-1 records.

6.2.3. Field 9.003: Impression type (IMP)

Dette obligatoriske en-byte felt beskriver, hvor informationen om fingeraftryksbilledet blev indsamlet. ASCII værdien af den korrekte kode, som valgt fra tabel 4, indlæses i dette felt for at angive aftrykstypen.

6.2.4. Field 9.004: Minutiæformat (FMT)

Dette felt indeholder et "U" for at angive, at minutiae er formatteret efter M1-378 standard. Selv om informationer kan kodes i overensstemmelse med M1-378 standarden, skal alle data i felter i type-9 records fortsat være ASCII tekstfelter.

6.2.5. Field 9.126: CBEFF information

Dette felt indeholder tre informationselementer. Det første informationselement skal indeholde værdien "27" (0x1B). Det er for at identificere ejeren af CBEFF-formatet, der af International Biometric Industry Association (IBIA) er udpeget til INCITS Technical Committee M1. <US>-tegnet skal adskille dette element fra CBEFF-formattypen, der har en værdi på "513" (0x0201) for at angive, at denne record kun indeholder data om placering og angulærretning uden nogen udvidet datablokinformation. <US>-tegnet skal adskille dette element fra CBEFF Product Identifier (PID), der identificerer "ejeren" af kodningsudstyret. Det er sælger, der fastsætter denne værdi. Det kan fås på IBIA's websted (www.ibia.org), hvis det er indlæst.

6.2.6. Field 9.127: Capture equipment identification

Dette felt indeholder to informationselementer, der er adskilt af <US> tegnet. Det første skal indeholde "APPF", hvis det udstyr, der oprindeligt blev anvendt til at tage billedet var certificeret i overensstemmelse med tillæg F (IAFIS Image Quality Specification af 29. januar 1999) i CJIS-RS-0010, Federal Bureau of Investigation's Electronic Fingerprint Transmission Specification. Hvis udstyret ikke var i overensstemmelse hermed, indeholder det værdien "NONE". Andet informationselement skal indeholde optagelsesudstyrets ID, som er sælgers produktnummer på optagelsesudstyret. Værdien "0" angiver, at optagelsesudstyrets ID ikke er registreret.

6.2.7. Field 9.128: Horizontal line length (HLL)

Dette obligatoriske ASCII felt angiver antallet af pixel i en enkelt horisontal linje i det overførte billede. Den maksimale horisontale størrelse er begrænset til 65,534 pixel.

6.2.8. Field 9.129: Vertical line length (VLL)

Dette obligatoriske ASCII felt skal indeholde antallet af horisontale linjer i det overførte billede. Den maksimale vertikale størrelse er begrænset til 65,534 pixel.

6.2.9. Field 9.130: Scale units (SLC)

Dette obligatoriske ASCII-felt angiver de enheder, der anvendes til at beskrive pixeltætheden. Et "1" i dette felt angiver pixel pr. inch og et "2" angiver pixel pr. centimeter. Et "0" i dette felt angiver, at der er ikke er angivet nogen skala. I dette tilfælde angiver kvotienten af HPS/VPS pixelaspektratioen.

6.2.10. Field 9.131: Horizontal pixel scale (HPS)

Dette obligatoriske ASCII-felt angiver den horisontale pixeltæthed i hele tal, der anvendes horisontalt, når SLC indeholder et "1" eller "2". Ellers angiver det den horisontale komponent af pixelaspektratioen.

6.2.10. Field 9.132: Vertical pixel scale (VPS)

Dette obligatoriske ASCII-felt angiver den vertikale pixeltæthed i hele tal, der anvendes vertikalt, når SLC indeholder et "1" eller et "2". Ellers angiver det den vertikale komponent af pixelaspektratioen.

6.2.11. Field 9.133: Finger view

Dette obligatoriske felt angiver viewnummeret på den finger, der er knyttet til denne records data. Nummeret begynder med "0" og stiger med en ad gangen til "15".

6.2.12. Field 9.134: Finger position (FGP)

Dette felt angiver koden for den fingerposition, der leverede oplysningen til denne type-9 record. En kode mellem 1 og 10 fra tabel 5 eller den relevante håndfladekode fra tabel 10 skal anvendes til at angive finger- eller håndfladepositionen.

6.2.13. Field 9.135: Finger quality

Dette felt angiver kvaliteten af de samlede minutiaedata for fingeren og angives mellem 0 og 100. Tallet giver et samlet overblik over kvaliteten af fingerrecorden og repræsenterer kvaliteten af det oprindelige billede, af minutiaene og andre yderligere operationer, der kan berøre minutiaerecorden.

6.2.14. Field 9.136: number of minutiæ

Dette obligatoriske felt indeholder en opregning af antallet af minutiae, der er registreret i denne logiske record.

6.2.15. Field 9.137: Finger minutiæ data

Dette obligatoriske felt har seks informationselementer adskilt af <US> tegnet. Det består af flere subfelter, som hver indeholder detaljer af de enkelte minutiae. Det samlede antal minutiaesubfelter skal svare til antallet i felt 136. Det første informationselement er indeksnummeret for minutiae, der indledes med "1" øges med "1" for hver yderligere minutiae i fingeraftrykket. Andet og tredje informationselement er x-koordinaten og y-koordinaterne i minutiae angivet i pixelenheder. Fjerde informationselement er minutiae-vinklen angivet i enheder på to grader. Denne værdi skal være ikke-negativ mellem 0 og 179. Femte informationselement er minutiae-typen. "0" angiver minutiae af typen "OTHER", "1" en linjeafslutning (ridge ending) og "2" en linjebifurcation. Sjette informationselement angiver kvaliteten af hver minutiae. Denne værdi går fra 1 som minimum og 100 som maksimum. "0" angiver, at der ikke er nogen kvalitetsværdi. Hvert subfelt adskilles fra det næste ved at anvende <RS> separatortegnet.

6.2.16. Field 9.138: Ridge count information

Dette felt består af en række subfelter, der hver især indeholder tre informationselementer. Det første element i første subfelt angiver metoden til ekstraktion af linjeantallet. "0" angiver, at det ikke vides, hvilken metode der er brugt til ekstraktion af linjeantallet eller deres rækkefølge i recorden. "1" angiver, at der for hver central minutiae blev ekstraheret data om linjeantal til nærmeste minutiae i fire kvadranter, og linjeantal for hver centrale minutiae opgives samlet. "2" angiver, at der for hver centrale minutiae blev ekstraheret data om linjeantal til nærmeste minutiae i otte oktanter, og linjeantal for hver centrale minutiae opgives samlet. De resterende to informationselementer i første subfelt skal begge indeholde "0". Informationselementer adskilles med <US>-separatortegnet. Efterfølgende subfelter vil indeholde indeksnummeret for den centrale minutiae som første informationselement, indeksnummeret for nærliggende minutiae som andet informationselement og antallet af linjer, der krydses, som tredje informationselement. Subfelter adskilles af <RS>-separatortegnet.

6.2.17. Field 9.139: Core information

Dette felt består af et subfelt for hver kerne i det oprindelige billede. Hvert subfelt består af tre informationselementer. De første to elementer indeholder x- og y-koordinatpositionerne i pixelenheder. Det tredje element indeholder kernens vinkel registreret i enheder på 2 grader. Værdien skal være en ikke-negativ værdi mellem 0 og 179. Flere kerner adskilles af <RS>-separatortegnet.

6.2.18. Field 9.140: Delta information (deltainformation)

Dette felt består af et subfelt for hvert delta i det oprindelige billede. Hvert subfelt består af tre informationselementer. De første to elementer indeholder x- og y-koordinatpositionerne i pixelenheder. Det tredje element indeholder deltaets vinkel registreret i enheder på 2 grader. Værdien skal være en ikke-negativ værdi mellem 0 og 179. Flere kerner vil blive adskilt af <RS>-separatortegnet.

7. Type-13 record - Latent billede med variabel opløsning

Type-13 logiske records med mærkede felter indeholder billeddata fra latente billeder. Disse billeder er beregnet på at blive overført til agenturer, der automatisk eller ved menneskelig indgriben og behandling vil ekstrahere de ønskede informationer om tegnene fra billederne. Information vedrørende scanningsopløsning, billedstørrelse og andre parametre, der kræves til at behandle billedet, registreres som mærkede felter i recorden.

Tabel: Type-13 record- Latent billede med variabel opløsning

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
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

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

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

7.1. Felter i type-13 logisk record

Følgende afsnit beskriver de data, der er indeholdt i hvert af felterne for type-13 logiske records.

I type-13 logiske records skal indlæsninger foretages i nummererede felter. Det er nødvendigt, at de to første felter i recorden står i samme rækkefølge, og feltet med billeddata skal være angivet i recordens sidste fysiske felt. For hvert felt i type-13 records indeholder tabel 7 feltet "condition code" som "mandatory" (obligatorisk) "M" eller "optional" (fakultativ) "O", feltnummer, feltnavn, tegntype, feltstørrelse og grænser for forekomst. Baseret på et trecifret feltnummer er det maksimale antal bytes angivet i sidste kolonne. Da der anvendes flere cifre til feltnummeret, vil det maksimale antal bytes også stige. De to felter i "field size per occurence" omfatter alle separatortegn, der anvendes i feltet. "Maximum byte count" omfatter feltnummer, oplysninger og alle separatortegn herunder også "GS".

7.1.1. Field 13.001: Logical record length (LEN)

Dette obligatoriske ASCII felt skal indeholde det samlede antal bytes i den logiske type-13 record. Felt 13.001 skal angive recordens længde og omfatte samtlige tegn i hvert felt samt informationsseparatorerne.

7.1.2. Field 13.002: Image designation character (IDC)

Dette obligatoriske ASCII-felt anvendes til at identificere de latente billeddata, der er indeholdt i recorden. Dette IDC skal matche det IDC, der findes i filindholdsfeltet (CNT) for type-1 record.

7.1.3. Field 13.003: Impression type (IMP)

Dette obligatoriske en-byte ASCII-felt angiver, hvordan de latente billeddata blev indsamlet. I dette felt indlæses den relevante latente kode fra tabel 4 (finger) eller tabel 9 (håndflade).

7.1.4. Field 13.004: Source agency ORI (SRC)

Dette obligatoriske ASCII-felt indeholder identifikationen af den administration eller organisation, der først indlæste ansigtsbilledet i recorden. Normalt vil feltet angive "the Originating Agency Identifier" (ORI) for det agentur, der tog billedet. Det består af to informationselementer i følgende format: CC/*agency*.

Det første element angiver Interpols landekode på to alfanumeriske tegn. Det andet element *agency* er en fritekstidentificering af agenturet på højt 32 alfanummeriske tegn.

7.1.5. Field 13.005: Latent capture date LCD)

Dette obligatoriske ASCII-felt angiver den dato, hvor den latente billede i recorden blev taget. Datoen er angivet med otte chifre i formatet CCYYMMDD. CCYY angiver det år, hvor billedet blev taget; MM angiver måneden; og DD angiver datoen. For eksempel angiver 20000229 den 29. februar 2000. Den fuldstændige dato skal være i et ægte datoformat

7.1.6. Field 13.006: Horizontal line length (HLL)

Dette obligatoriske ASCII-felt angiver antallet af pixel i en enkelt horisontal linje af det overførte billede.

7.1.7. Field 13.007: Vertical line length (VLL)

Dette obligatoriske ASCII-felt angiver antallet af horisontale linjer i det overførte billede.

7.1.8. Field 13.008: Scale units (SLC)

Dette obligatoriske ASCII-felt angiver de enheder, der anvendes til at beskrive pixeltætheden. Et "1" i dette felt angiver pixel pr. inch og et "2" angiver pixel pr. centimeter. Et "0" i dette felt angiver, at der er ikke er angivet nogen skala. I dette tilfælde angiver kvotienten af HPS/VPS pixelaspektratioen.

7.1.9. Field 13.009: Horizontal pixel scale (HPS)

Dette obligatoriske ASCII-felt angiver den horisontale pixeltæthed i hele tal, når SLC indeholder et "1" eller "2". Ellers angiver det den horisontale komponent af pixelaspekt-ratioen.

7.1.10. Field 13.010: Vertical pixel scale (VPS)

Dette obligatoriske ASCII-felt angiver den vertikale pixeltæthed i hele tal, når SLC indeholder et "1" eller et "2". Ellers angiver det den vertikale komponent af pixelaspekt-ratioen.

7.1.11. Field 13.011: Compression algorithm (CGA)

Dette obligatoriske ASCII-felt angiver den algoritme, der anvendes til at komprimere gråtonebilleder. Gyldige kompressionskoder findes i tillæg 7.

7.1.12. Field 15.012: Bits per pixel (BPX)

Dette obligatoriske ASCII-felt angiver antal bits pr. pixel. I feltet angiver "8" normale gråtoneværdier fra "0" til "255". Hvis der i dette felt indlæses en værdi højere eller lavere end "8" repræsenterer det en gråtoneværdi med henholdsvis større eller mindre præcision.

7.1.13. Field 13.013: Finger/palm position (PLP)

Dette obligatoriske mærkede felt angiver en eller flere finger- eller håndfladepositioner, der kan matche det latente billede. Decimalkodenummeret, der svarer til den kendte eller mest sandsynlige fingerposition, tages fra tabel 5 eller den mest sandsynlige håndfladeposition fra tabel 10 og indlæses som et et- eller tocifret ASCII-subfelt. Der kan henvises til supplerende finger- og/eller håndfladepositioner ved at indlæse de alternative positionskoder som subfelter adskilt af "RS" separatortegnet. Kode "0" for "Unknown Finger" (ukendt finger) anvendes til at henvise til fingerposition 1-10. Kode "20" for "Unknown Palm (ukendt håndflade) anvendes til at henvise til alle opførte håndfladeaftrykspositioner.

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

Disse felter er reserveret til indlæsning af kommende revisioner af denne standard. Ingen af disse felter må anvendes på nuværende revisionsniveau. Hvis disse felter forekommer, skal de ignoreres.

7.1.15. Field 13.020: Comment (COM)

Dette fakultative felt kan anvendes til at indlæse bemærkninger eller anden ASCII-tekstinformation sammen med data vedrørende håndfladeaftryksdata.

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

Disse felter er reserveret til indlæsning af kommende revisioner af denne standard. Ingen af disse felter må anvendes på nuværende revisionsniveau. Hvis disse felter forekommer, skal de ignoreres.

7.1.17. Field 13.200-998: User-defined fields (UDF)

Disse felter kan defineres af brugerne og vil blive anvendt til fremtidige krav. Deres størrelse og indhold defineres af brugeren efter aftale med det modtagende agentur. Hvis disse felter forekommer, skal de indeholde ASCII-tekstinformation

7.1.18. Field 13.999: Image data (DAT)

Dette felt indeholder alle data fra et håndfladeaftryksbillede. Det skal altid have feltnummer 999 og være det sidste fysiske felt i recorden. For eksempel efterfølges "13.999:" af billeddata i binær repræsentation.

Hver pixel af ukomprimerede gråtonedata skal normalt angives med otte bits (256 gråtoneniveauer) indeholdt i en enkelt byte. Hvis indlæsningen i BPX Felt 13.012 er højere eller lavere end 8, vil det antal bytes, der kræves til at indeholde en pixel, være forskelligt. Hvis der anvendes kompression, skal pixeldataene komprimeres i overensstemmelse med den kompressionsteknisk, der er angivet i CGA-feltet.

7.2. Afslutning af type-13 record: latente billeder med variabel opløsning

Af hensyn til sammenhængen skal der umiddelbart efter den sidste databyte i felt 13.999 indsættes en "FS"-separator for at adskille den fra den næste logiske record. Denne separator skal indlæses i længdefeltet i type-13 recorden.

8. Type-15 record - Håndfladeaftryk med variabel opløsning

Type-15 logisk record med mærkede felter indeholder og anvendes til at udveksle håndfladeaftryksbilleddata sammen med fastlagte og brugerdefinerede tekstinformationsfelter, der er relevante for det digitaliserede billede. Information om scanningopløsning, billedstørrrelse og andre parametre eller bemærkninger, der kræves til at behandle billedet, registreres som mærkede felter i recorden. Håndfladeaftryksbilleder, der overføres til andre agenturer vil blive behandlet af modtageragenturerne, så de kan ekstrahere de informationstegn, der kræves med henblik på matchning. Billeddataene fås direkte fra en person, der anvender live scan-udstyr, eller fra en håndfladeaftryksformular eller andre medier, der indeholder personens håndfladeaftryk.

Enhver metode til at optage håndfladeaftryksbilleder skal kunne tage et sæt af billeder for hver hånd. Dette sæt skal omfatte lillefingerbalden som et enkelt scannet billede og hele håndfladen fra håndleddet til fingerspidserne som et eller to scannede billeder. Hvis der anvendes to billeder til at repræsentere hele håndfladen, skal det nederste billede gå fra håndleddet til toppen af interdigitalregionen (tredje fingerled) og omfatte tenar- og hypotenarregionen i håndfladen. Det øverste billede skal gå fra den nederste del af interdigitalregionen til de yderste fingerspidser. Dette giver et passende antal overlapninger mellem de to billeder, som begge findes over håndfladens interdigitalregion. Ved at sammenholde linjestrukturer og detaljer i dette fælles område, kan en undersøger med sikkerhed konstatere, om begge billeder kommer fra samme håndflade.

Da en håndfladeaftrykstransaktion kan anvendes til forskellige formål, kan den indeholde et eller flere unikke billedområder optaget fra håndfladen eller hånden. Et fuldstændigt recordsæt af håndfladeaftryk for en enkelt person vil normalt omfatte lillefingerbalden og det/de fulde håndfladebillede(r) fra hver hånd. Da logiske billed-records med mærkede felter kun kan indeholde et binært felt, kræves der en enkelt type-15 record for hver lillefingerbalde og en eller to type-15 record(s) for hver fulde håndflade. Derfor kræves der 4-6 type-15 record til at repræsentere personens håndfladeaftryk i en normal håndfladeaftrykstransaktion.

8.1. Felter i type-15 logisk record

I de følgende afsnit beskrives de data, der er indeholdt i hvert af felterne i type-15 logiske records. I type-15 logiske records skal indlæsninger foretages i nummererede felter. Det er nødvendigt, at de to første felter i recorden står i samme rækkefølge, og feltet med billeddata skal være angivet i recordens sidste fysiske felt. For hvert felt i type-15 records indeholder tabel 8 feltet "condition code", som værende "mandatory" (obligatorisk) "M" eller "optional" (fakultativ) "O", feltnummer, feltnavn, tegntype, feltstørrelse og grænser for forekomst. Baseret på et trecifret feltnummer er det maksimale antal bytes angivet i sidste kolonne. Da der anvendes flere cifre til feltnummeret, vil det maksimale antal bytes også stige. De to felter i "field size per occurence" omfatter alle separatortegn, der anvendes i feltet. "Maximum byte count" omfatter feltnummer, oplysninger og alle separatortegn herunder også "GS".

8.1.1. Field 15.001: Logical record length (LEN)

Dette obligatoriske ASCII felt skal indeholde det samlede antal bytes i den logiske type 15 record. Felt 15.001 skal angive recordens længde og omfatte samtlige tegn i hvert eneste felt samt informationsseparatorerne.

8.1.2. Field 15.002: Image designation character (IDC)

Dette obligatoriske ASCII-felt anvendes til at identificere det håndfladeaftryksbillede, der er indeholdt i recorden. Dette IDC skal matche det IDC, der blev fundet i filindholdsfeltet (CNT) i type-1 record.

8.1.3. Field 15.003: Impression type (IMP)

Dette obligatoriske en-byte ASCII-felt angiver, hvordan informationen om håndfladeaftryksbilledet blev indsamlet. I dette felt indlæses den relevante kode fra tabel 9.

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

Dette obligatoriske ASCII-felt indeholder identifikationen af den administration eller organisation, der først indlæste ansigtsbilledet i recorden. Normalt vil feltet angive "the Originating Agency Identifier" (ORI) for det agentur, der tog billedet. Det består af to informationselementer i følgende format: CC/*agency*.

Det første element angiver Interpols landekode på to alfanumeriske tegn. Det andet element *agency* (agentur) er en fritekstidentificering af agenturet på højt 32 alfanumeriske tegn.

8.1.5. Field 15.005: Palmprint capture date (PCD)

Dette obligatoriske ASCII-felt angiver den dato, hvor håndfladeaftrykket blev taget. Datoen er angivet med otte chifre i formatet CCYYMMDD. CCYY angiver det år, hvor billedet blev taget; MM angiver måneden; og DD angiver datoen. For eksempel angiver 20000229 den 29. februar 2000. Den fuldstændige dato skal være i et ægte datoformat

8.1.6. Field 15.006: Horizontal line length (HLL)

Dette obligatoriske ASCII-felt angiver antallet af pixel i en enkelt horisontal linje af det overførte billede.

8.1.7. Field 15.007: Vertical line length (VLL)

Dette obligatoriske ASCII-felt angiver antallet af horisontale linjer i det overførte billede.

8.1.8. Field 15.008: Scale units (SLC)

Dette obligatoriske ASCII-felt angiver de enheder, der anvendes til at beskrive pixeltætheden. Et "1" i dette felt angiver pixel pr. inch og et "2" angiver pixel pr. centimeter. Et "0" i dette felt angiver, at der er ikke er angivet nogen skala. I dette tilfælde angiver kvotienten af HPS/VPS pixelaspektratioen.

8.1.9. Field 15.009: Horizontal pixel scale (HPS)

Dette obligatoriske ASCII-felt angiver den horisontale pixeltæthed i hele tal, når SLC indeholder et "1" eller "2". Ellers angiver det den horisontale komponent af pixelaspektratioen.

8.1.10. Field 15.010: Vertical pixel scale (VPS)

Dette obligatoriske ASCII-felt angiver den vertikale pixeltæthed i hele tal, når SLC indeholder et "1" eller et "2". Ellers angiver det den vertikale komponent af pixelaspektratioen.

Tabel 8: Type-15 record: håndefladeaftryk med variabel opløsning

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

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE INCLUSION	--	--	--	--	--	--
COM	O	15.020	COMMENT	AN	2	128	0	1	128
RSV		15.021 15.199	RESERVED FOR FUTURE INCLUSION	--	--	--	--	--	--
UDF	O	15.200 15.998	USER-DEFINED FIELDS	--	--	--	--	--	--
DAT	M	15.999	IMAGE DATA	B	2	--	1	1	--

Tabel 9: Håndfladeaftrykstype

Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11. Field 15.011: Compression algorithm (CGA)

Dette obligatoriske ASCII-felt angiver den algoritme, der anvendes til at komprimere gråtonebilleder. Hvis der indlæses et "NONE" i dette felt angiver det, at dataene i denne record ikke er komprimerede. For de billeder, der skal komprimeres, indeholder feltet den foretrukne metode til at komprimere tenprint fingeraftryksbilleder.

Gyldige kompressionskoder findes i bilag 7.

8.1.12. Field 15.012: Bits per pixel (BPX)

Dette obligatoriske ASCII-felt angiver antal bits pr. pixel. I feltet angiver "8" normale gråtoneværdier fra "0" til "255". Hvis der i dette felt indlæses en værdi højere eller lavere end "8" repræsenterer det en gråtoneværdi med henholdsvis større eller mindre præcision.

Tabel 10: Håndfladekoder, områder og størrelser

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

8.1.13. Field 15.013: Palmprint position (PLP)

Dette obligatoriske mærkede felt angiver håndfladeaftrykkets position, der matcher håndfladeaftryksbilledet. Decimalkodenummeret, der skal svare til den kendte eller mest sandsynlige håndfladeaftrykspositon, tages fra tabel 10 og indlæses som et tocifret ASCII-subfelt. Tabel 10 angiver også de maksimale billedområder og -dimensioner for hver af de mulige håndfladeaftrykspositioner.

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

Disse felter er reserveret til indlæsning af kommende revisioner af denne standard. Ingen af disse felter må anvendes på nuværende revisionsniveau. Hvis disse felter forekommer, skal de ignoreres.

8.1.15. Field 15.020: Comment (COM)

Dette fakultative felt kan anvendes til at indlæse bemærkninger eller anden ASCII-tekstinformation sammen med data vedrørende håndfladeaftryksdata.

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

Disse felter er reserveret til indlæsning af kommende revisioner af denne standard. Ingen af disse felter må anvendes på nuværende revisionsniveau. Hvis disse felter forekommer, skal de ignoreres.

8.1.17. Field 15.200-998: User-defined fields (UDF)

Disse felter kan defineres af brugerne og vil blive anvendt til fremtidige krav. Deres størrelse og indhold defineres af brugeren efter aftale med det modtagende agentur. Hvis disse felter forekommer, skal de indeholde ASCII-tekstinformation

8.1.18. Field 15.999: Image data (DAT)

Dette felt indeholder alle data fra et håndfladeaftryksbillede. Det skal altid have feltnummer 999 og skal være det sidste fysiske felt i recorden. For eksempel efterfølges "15.999:" af billeddata i binær repræsentation. Hver pixel af ukomprimerede gråtonedata skal normalt angives med otte bits (256 gråtoneniveauer) indeholdt i en enkelt byte. Hvis indlæsningen i BPX Felt 15.012 er højere eller lavere end 8, vil det antal bytes, der kræves til at indeholde en pixel, være forskelligt. Hvis der anvendes kompression, skal pixeldataene komprimeres i overensstemmelse med den kompressionsteknik, der er angivet i CGA-feltet.

8.2. Afslutning af type-15 record: håndefladeaftryk med variabel opløsning

Af hensyn til sammenhængen skal der umiddelbart efter den sidste databyte i felt 15.999 indsættes en "FS"-separator for at adskille den fra den næste logiske record. Denne separator skal indlæses i længdefeltet i type-15 recorden.

8.3. Supplerende type-15 record: håndefladeaftryk med variabel opløsning

Der kan indlæses yderligere type-15 records i denne fil. For hvert supplerende håndfladeaftryksbillede kræves der en komplet type-15 logisk record sammen med en "FS"-separator.

Tabel 11: Det maksimale antal personer, der accepteres med henblik på kontrol pr. overførsel

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

Søgningstyper:

TP/TP: ten-print against ten-print

LT/TP: fingerprint latent against ten-print

LP/PP: palmprint latent against palmprint

TP/UL: ten-print against unsolved fingerprint latent

LT/UL: fingerprint latent against unsolved fingerprint latent

PP/ULP: palmprint against unsolved palmprint latent

LP/ULP: palmprint latent against unsolved palmprint latent

9. Tillæg til kapitel 2 (udveksling af fingeraftryksoplysninger)

9.1. Tillæg 1 ASCII Separatorkoder

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

9.2. Tillæg 2 Beregning af alfanumeriske kontroltegn

For TCN og TCR (Felt 1.09 og 1.10):

Det tal, der svarer til kontroltegnet, findes ved at anvende følgende formel:

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

Hvor YY og SSSSSSSS er numeriske værdier for henholdsvis de sidste to cifre for året og serienummeret.

Kontroltegnet findes herefter i opslagstabellen nedenfor.

For CRO (Felt 2.010)

Det tal, der svarer til kontroltegnet, findes ved at anvende følgende formel:

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

Hvor YY og NNNNNN er numeriske værdier for henholdsvis de to sidste cifre for året og serienummeret.

Kontroltegnet findes herefter i opslagstabellen nedenfor.

---

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

Opslagstabel for kontroltegn

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. Tillæg 3 Tegnkoder

7-bit ANSI-kode for informationsudveksling

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. Tillæg 4 Transaktionsresumé

Type-1 Record (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
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

I kolonnen "Condition":

O = Optional (fakultativ); M = Mandatory (obligatorisk); C = Conditional (betinget), hvis transaktionen er et svar til det anmodende agentur

Type-2 Record (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	-	-

I kolonnen "Condition":

O = Optional (fakultativ); M = Mandatory (obligatorisk; C = Conditional (betinget) (afhængigt af, om dataene er tilgængelige

*) = hvis transmissionen af dataene er i overensstemmelse med national lovgivning (der ikke er omfattet af Rådets afgørelse 2007/.../RIA)

9.5. Tillæg 5 Definitioner i type-1 record

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{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

I kolonnen "Condition": O= Optional (fakultativ), M= Mandatory (obligatorisk), C= Conditional (betinget)

I kolonnen Character Type: A= Alpha, N= Numeric, B= Binary

1* tilladte tegn for agenturnavn er ["0..9", "A..Z", "a..z", "_", ".", " ", "-"]

9.6. Tillæg 6 Definitioner af type-2 records

Tabel A.6.1: CPS- og 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}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Tabel A.6.2: SRE-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}

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

Tabel A.6.4: MPS- og 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}

I kolonnen "Condition": O= Optional (fakultativ), M= Mandatory (obligatorisk), C= Conditional (betinget)

I kolonnen Character Type (tegntype): A= Alpha, N= Numeric, B= Binary

1* tilladte tegn er: ["0..9", "A..Z", "a..z", "_", ".", " ", "-", ","]

9.7. Tillæg 7 Gråtonekompressionskoder

Kompressionskoder

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

9.8. Tillæg 8 Mailspecifikation

For at forbedre den interne workflow skal "mailsubject" for en PRUEM-transaktion udfyldes med landekoden (CC) for den medlemsstat, der sender mailen og transaktionstypen (TOT Felt 1.004).

Format: CC/*type of transaction*

Eksempel: "DE/CPS"

Mailens tekstfelt kan være tomt.

Kapitel 3: Udveksling af oplysninger fra køretøjsregistre

1. Fælles data med henblik på elektronisk søgning af oplysninger fra køretøjsregistre

1.1. Definitioner

Definitionerne af henholdsvis de obligatoriske og de fakultative dataelementer, jf. artikel 16, stk. 4, er som følger:

Obligatoriske (Mandatory (M)):

Dataelementet skal meddeles, når oplysningerne er tilgængelig i en medlemsstats nationale register. Der er altså en **forpligtelse** til at udveksle oplysningerne, **hvis de er tilgængelige**.

Fakultative (Optional (O)):

Dataelementet kan meddeles, når oplysningerne er tilgængelige i en medlemsstats nationale register. Der er altså **ingen forpligtelse** til at udveksle oplysningerne, selv om de er tilgængelige.

For hvert dataelement markeres det med 'Y', hvis elementet udtrykkelig er udpeget som betydningsfuldt i henhold til afgørelse 2008/.../RIA.

1.2. Søgen efter køretøj/ejer/bruger

1.2.1. Søgeelementer

Der findes to forskellige måder at søge de oplysninger, der er anført i det følgende afsnit.

- via stelnummer (VIN), referencedato og -tidspunkt (fakultativt)
- via registreringsnummer, stelnummer (VIN) (kan udelades), referencedato og -tidspunkt (fakultativt).

Ved søgning ud fra disse kriterier fås oplysninger om et enkelt og i visse tilfælde flere køretøjer. Hvis der kun fås oplysninger om et enkelt køretøj, gives alle oplysningerne som **et samlet** svar. Hvis der findes mere end et køretøj, kan den anmodede stat selv bestemme, hvilke oplysninger der skal gives: alle oplysningerne eller kun oplysninger til indskrænkning af søgningen (f.eks. af hensyn til privatlivets fred eller af tekniske årsager).

Afsnit 1.2.2.1 omhandler de oplysninger, der er nødvendige for at indskrænke søgningen. Afsnit 1.2.2.2 omhandler samtlige oplysninger.

Hvis der søges via stelnummer samt referencedato og -tidspunkt, kan søgningen omfatte **en eller alle** de deltagende medlemsstater.

Hvis der søges via registreringsnummer samt referencedato og -tidspunkt, skal søgningen omfatte **en bestemt** medlemsstat.

Normalt søges der med gældende dato og tidspunkt, men det er muligt at foretage søgninger med referencedatoer og -tidspunkter i fortiden. Hvis der søges med en referencedato og et referencetidspunkt i fortiden, og der ikke foreligger historiske oplysninger i den pågældende medlemsstats registre, fordi sådanne oplysninger slet ikke registreres, kan de gældende oplysninger fås med angivelse af, at det drejer sig om gældende oplysninger.

1.2.2. Data

1.2.2.1. Oplysninger, der er nødvendige for at indskrænke søgningen

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**
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, 29-04-1999.

1.2.2.2. Komplette datasæt

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	N

1 M = mandatory when available in national register, O = optional.
2 Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999.

Item	M/O[1]	Remarks	Prüm Y/N
		number).	
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**
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

Item	M/O[1]	Remarks	Prüm Y/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[1]	O	A second document ID as printed on the vehicle document.	**Y**

[1] In Luxembourg two separate vehicle registration document ID's are used.

Item	M/O[1]	Remarks	Prüm Y/N
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
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

2. Datasikkerhed

2.1. Oversigt

Eucaris-softwareprogrammet sørger for sikker kommunikation med de øvrige medlemsstater og kommunikerer til medlemsstaternes back-end legacy-systemer via XML. Medlemsstaterne udveksler meddelelser ved at sende dem direkte til modtageren. Den enkelte medlemsstats datacenter er forbundet med EU's Testa-net.

XML-meddelelser, der sendes over nettet, er krypteret. Teknikken til kryptering af disse meddelelser er SSL. De meddelelser, der sendes til back-end, er XML-meddelelser med almindelig tekst, eftersom forbindelsen mellem programmet og back-end etableres i et beskyttet miljø.

Der stilles et klientprogram til rådighed, som kan bruges inden for en medlemsstat til søgning i eget register eller andre medlemsstaters registre. Klienterne identificeres ved hjælp af et bruger-id/en adgangskode eller et brugercertifikat. Forbindelsen til en bruger kan være krypteret, men dette har den enkelte medlemsstat ansvaret for.

2.2. Sikkerhedsfeatures i forbindelse med udveksling af meddelelser

Sikkerhedssystemet er udformet som en kombination af HTTPS og XML-signatur. Dette alternativ benytter en XML-signatur til at underskrive alle meddelelser, der sendes til serveren, og kan autentificere afsenderen ved kontrol af signaturen. Ensidig SSL (kun servercertifikat) bruges til at beskytte meddelelsens fortrolighed og integritet under overførslen og beskytter mod sletnings-/replay- og indsætningsangreb. I stedet for skræddersyet software-udvikling til implementering af tosidet SSL, implementeres en XML-signatur. Brug af XML-signatur svarer bedre til køreplanen for webtjenester end tosidet SSL og er derfor mere strategisk.

XML-signaturen kan implementeres på flere måder, men den valgte tilgang er at anvende XML-signaturen som del af Web Services Security (WSS). WSS specificerer, hvordan XML-signaturen skal anvendes. Da WSS bygger på SOAP-standarden, er det logisk så vidt muligt at overholde denne standard.

2.3. Sikkerhedsfeatures uden forbindelse med udveksling af meddelelser

2.3.1. Brugerautentificering

Brugerne af Eucaris-webprogrammet autentificerer sig ved hjælp af et brugernavn og en adgangskode. Da der anvendes standard-Windows-autentificering, kan medlemsstaterne om nødvendigt etablere et højere niveau af brugerautentificering ved at anvende brugercertifikater.

2.3.2. Brugerroller

Eucaris-softwareprogrammet giver mulighed for forskellige brugerroller. Hver gruppe af tjenester kræver en speciel autorisation. F.eks. kan brugere, der (udelukkende) anvender Eucaristraktatfunktionen, ikke anvende Prümfunktionen. Administratortjenester er adskilt fra de almindelige slutbrugerroller.

2.3.3. Logføring og sporing af udveksling af meddelelser

Eucaris-softwareprogrammet gør det nemt at logføre alle typer meddelelser. En administratorfunktion giver den nationale administrator mulighed for at afgøre, hvilke meddelelser der skal logføres: anmodninger fra slutbrugere, indkommende anmodninger fra andre medlemsstater, oplysninger, der er meddelt fra de nationale registre osv.

Programmet kan konfigureres til at anvende enten en intern database til denne logføring eller en ekstern (Oracle) database. Beslutningen om, hvilke meddelelser der skal logføres, afhænger naturligvis af logfaciliteterne andre steder i legacysystemerne og de dermed forbundne brugerprogrammer.
Den enkelte meddelelses teksthoved indeholder oplysninger om den anmodende medlemsstat, den anmodende organisation i den pågældende medlemsstat og den berørte bruger. Årsagen til anmodningen er også anført.
Ved at sammenholde logføringen i de medlemsstater, der henholdsvis anmoder og besvarer anmodningen, er det muligt fuldt ud at spore alle udvekslinger af meddelelser (f.eks. efter anmodning fra en berørt borger).

Logføringen konfigureres ved hjælp af Eucaris web client (menu Administration, Logging configuration). Logføringsfunktionen udføres af det centrale system (Core System). Når logføring er aktiveret, lagres hele meddelelsen (teksthovedet og selve teksten) i en enkelt logpost. Logføringsniveauet kan indstilles i forhold til de definerede tjenester og de meddelelsestyper, der går gennem det centrale system.

Logføringsniveauer

Følgende logføringsniveauer er mulige:
Privat - meddelelsen logføres: Logføringen er IKKE tilgængelig for udtræk fra logføringstjenesten, men er kun tilgængelig på nationalt niveau med henblik på audit og problemløsning.
Intet - meddelelsen logføres slet ikke.

Meddelelsestyper

Udvekslingen af oplysninger mellem medlemsstaterne omfatter flere forskellige meddelelser; i nedenstående skema findes en skematisk fremstilling af disse.
De mulige meddelelsestyper (i skemaet vist for Eucaris-centralsystemet i medlemsstat X) er som følger:

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

Følgende udvekslinger af oplysninger vises i diagrammet:

- Anmodning om oplysninger fra medlemsstat X til medlemsstat Y – blå pile. Denne anmodning og besvarelse omfatter henholdsvis meddelelsestype 1, 2, 7 og 6.
- Anmodning om oplysninger fra medlemsstat Z til medlemsstat X – røde pile. Denne anmodning og besvarelse omfatter henholdsvis meddelelsestype 3, 4, 9 og 8.
- Anmodning om oplysninger fra legacyregisteret til eget centralsystem (heri kan også indgå en anmodning fra en specielt udviklet klient længere tilbage end legacy-registeret) – grønne pile. Denne type anmodning omfatter meddelelsestype 5 og 10.

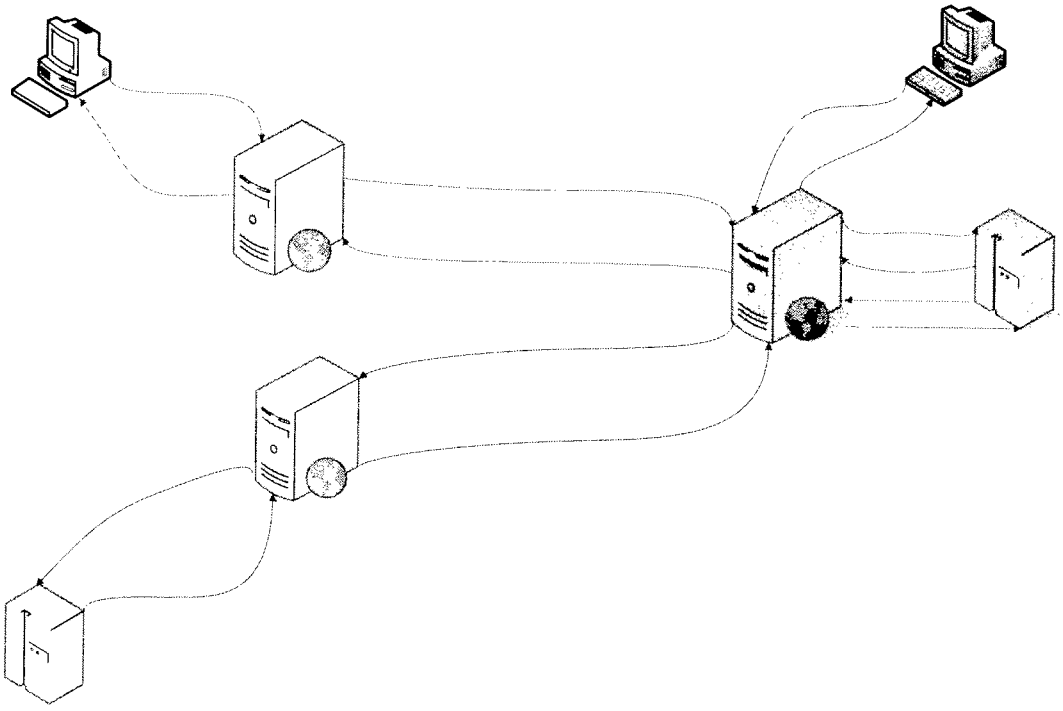


Diagram : Meddelelsestyper, der logføres

2.3.4. Hardwaresikkerhedsmodul

Der anvendes ikke et hardwaresikkerhedsmodul.

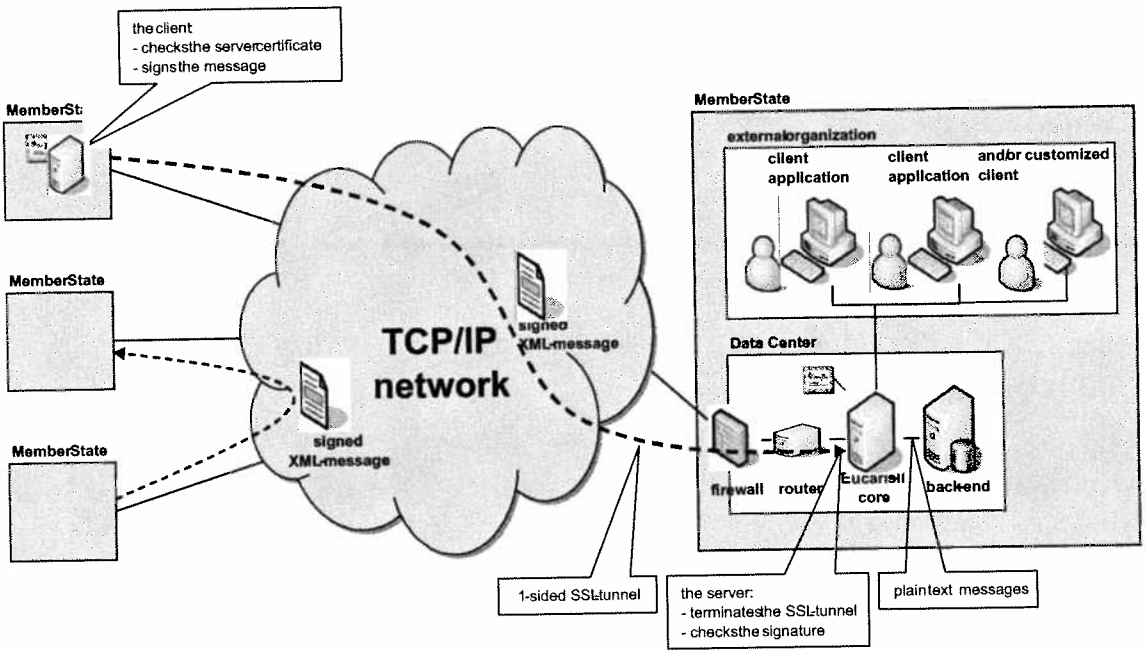
Et hardwaresikkerhedsmodul (HSM) giver god beskyttelse af den nøgle, der bruges til at signere meddelelser og identificere servere. Dette øger det samlede sikkerhedsniveau, men et HSM er dyrt at købe/vedligeholde, og der er ingen krav om at anskaffe et FIPS 140-2 niveau 2 eller niveau 3 HSM. Eftersom der anvendes et lukket net, der effektivt begrænser trusler, har man som udgangspunkt besluttet ikke at anvende et HSM. Hvis et HSM er nødvendigt, f.eks. for at opnå akkreditering, kan det tilføjes til systemarkitekturen.

3. De tekniske betingelser for dataudvekslingen

3.1. Generel beskrivelse af Eucarisprogrammet

3.1.1. Oversigt

Eucarisprogrammet forbinder alle de deltagende medlemsstater i et fuldmasket net, hvor hver medlemsstat kommunikerer direkte med en anden medlemsstat. Der er ikke behov for en central komponent for at etablere kommunikationen. Eucarisprogrammet formidler sikker kommunikation til de øvrige medlemsstater og kommunikerer til medlemsstaternes back-end legacy-systemer med brug af XML. Nedenstående tegning anskueliggør denne konstruktion.



Medlemsstaterne udveksler meddelelser ved at sende dem direkte til modtageren. Den enkelte medlemsstats datacenter er forbundet med det net, der anvendes til udveksling af meddelelser (Testa). For at få adgang til Testanettet, kobler medlemsstaterne sig på Testa via deres nationale adgangsportal. Der skal anvendes en firewall ved opkobling til nettet, og en router forbinder Eucarisprogrammet med firewallen. Afhængigt af, hvilken form for beskyttelse af meddelelserne man har valgt, udstedes et certifikat enten af routeren eller af Eucarisprogrammet.

Der stilles et klientprogram til rådighed, som kan bruges inden for en medlemsstat til søgning i eget register eller andre medlemsstaters registre. Klientprogrammet kobles til Eucaris. Klienterne identificeres ved hjælp af et bruger-id/en adgangskode eller et brugercertifikat. Forbindelsen til en bruger i en ekstern organisation (f.eks. politiet) kan være krypteret, men dette har den enkelte medlemsstat ansvaret for.

3.1.2. Systemets anvendelsesområde

Eucarissystemets anvendelsesområde er begrænset til de processer, der indgår i udveksling af oplysninger mellem medlemsstaternes registreringsmyndigheder og en simpel præsentation af disse oplysninger. Procedurer og elektroniske processer, hvor disse oplysninger skal anvendes, falder uden for systemets anvendelsesområde.

Medlemsstaterne kan vælge enten at anvende Eucarisklientfunktionen eller at udarbejde deres eget specielt udviklede klientprogram. I nedenstående skema gøres der rede for, hvilke aspekter af Eucarissystemet der er obligatoriske og/eller anbefales, og hvilke der er fakultative og/eller frit kan fastsættes af medlemsstaterne.

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

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

EUCARIS aspects	**M/O** [1]	**Remark**
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.

3.2. Funktionelle og ikke-funktionelle krav

3.2.1. Generiske funktioner

I denne sektion er de vigtigste generiske funktioner beskrevet i generelle vendinger.

Nr.	Beskrivelse
1.	Systemet giver medlemsstaternes registreringsmyndigheder mulighed for interaktivt at udveksle meddelelser med anmodninger og besvarelser.
2.	Systemet omfatter et klientprogram, der giver slutbrugerne mulighed for at sende anmodninger, og som præsenterer svaroplysningerne med henblik på manuel behandling.
3.	Systemet giver mulighed for "brede" henvendelser, så en medlemsstat kan sende en anmodning til alle de øvrige medlemsstater. De indkommende besvarelser konsolideres af det centrale program til en enkelt svarmeddelelse til klientprogrammet (denne funktionalitet kaldes en 'Multiple Country Inquiry').
4.	Systemet kan håndtere forskellige typer meddelelser. Brugerroller, autorisation, routing, signering og logføring er defineret for hver specifik tjeneste.
5.	Systemet giver medlemsstaterne mulighed for at udveksle bundter af meddelelser eller meddelelser, der indeholder et stort antal anmodninger eller besvarelser. Disse meddelelser behandles asynkront.
6.	Systemet sætter asynkrone meddelelser i kø, hvis modtagerstaten midlertidigt ikke kan kontaktes, og garanterer levering, så snart modtageren er tilgængelig igen.
7.	Systemet lagrer indkommende asynkrone meddelelser, indtil de kan behandles.
8.	Systemet giver kun adgang til de øvrige medlemsstaters Eucarisprogrammer, ikke til individuelle organisationer i disse medlemsstater, dvs. den enkelte registreringsmyndighed fungerer som eneste gateway mellem egne nationale slutbrugere og de tilsvarende myndigheder i de øvrige medlemsstater.
9.	Det er muligt på en Eucarisserver at definere brugere fra forskellige medlemsstater og give dem autorisation i henhold til den pågældende medlemsstats rettigheder.
10.	Oplysninger om den anmodende medlemsstat, organisation og slutbruger er indeholdt i meddelelserne.
11.	Systemet giver mulighed for logføring af udveksling af meddelelser mellem de forskellige medlemsstater og mellem det centrale program og de nationale registreringssystemer.

Nr.	Beskrivelse
12.	Systemet giver en særlig sekretær, som er en organisation eller en medlemsstat, der udtrykkelig er udpeget til denne opgave, mulighed for at indsamle oplysninger om meddelelser, der er afsendt/modtaget af alle de deltagende medlemsstater, med henblik på udarbejdelse af statistiske opgørelser.
13.	Hver enkelt medlemsstat anfører selv, hvilke logførte oplysninger der er stillet til rådighed for sekretæren, og hvilke oplysninger der er 'private'.
14.	Systemet tillader den enkelte medlemsstats nationale administratorer at uddrage statistikker om brugen.
15.	Systemet muliggør tilføjelse af nye medlemsstater ved hjælp af enkle administrative procedurer.

3.2.2. Anvendelighed

Nr.	Beskrivelse
16.	Systemet tilbyder en grænseflade (interface) for elektronisk behandling af meddelelser udført af back-end-systemer/legacy og giver mulighed for, at brugergrænsefladen integreres i disse systemer (specielt udviklet brugergrænseflade).
17.	Systemet er nemt at lære, selvforklarende og indeholder hjælpetekst.
18.	Systemet indeholder dokumentation, der kan bistå medlemsstaterne med integrering, operative aktiviteter og fremtidig vedligeholdelse (f.eks. referencevejledninger, dokumentation vedrørende funktionsmåde/teknisk dokumentation, brugervejledning,….).
19.	Brugergrænsefladen er flersproget og giver slutbrugeren mulighed for at vælge et foretrukket sprog.
20.	Brugergrænsefladen har faciliteter, så en lokal administrator kan oversætte både skærmtekst og kodede oplysninger til det nationale sprog.

3.2.3. Driftssikkerhed

Nr.	Beskrivelse
21.	Systemet er udformet som et robust og pålideligt operativt system, der er modstandsdygtigt over for operatørfejl og kan genetableres fuldt ud efter strømafbrydelser eller andre uheld. Det skal være muligt at genstarte systemet uden datatab eller med minimale datatab.
22.	Systemet skal give stabile og reproducerbare resultater.
23.	Systemet er udformet til at fungere stabilt. Det er muligt at implementere systemet i en konfiguration, der garanterer 98% tilgængelighed (ved hjælp af redundans, brug af backup-servere osv.) ved enhver bilateral kommunikation.

Nr.	Beskrivelse
24.	Det er muligt at bruge en del af systemet, selv om visse komponenter ikke fungerer (hvis medlemsstat C har nedbrud, kan medlemsstat A og B stadig kommunikere). Antallet af lokale fejl "single points of failure" i informationskæden bør holdes på et minimum.
25.	Genetableringstiden efter et alvorligt nedbrud bør være mindre end en dag. Det bør være muligt at minimere nedbrudsperioden ved hjælp af fjernsupport, f.eks. via en central servicetjeneste.

3.2.4. Ydeevne

Nr.	Beskrivelse
26.	Systemet kan anvendes døgnet rundt alle ugens dage (24x7). Det forudsættes dermed også, at medlemsstaternes legacysystemer er tilgængelige 24x7.
27.	Systemet reagerer hurtigt på anmodninger fra brugere uanset eventuelle baggrundsopgaver. Dette kræves også af parternes legacysystemer, så der sikres en acceptabel svartid. En samlet svartid på max. 10 sekunder for en enkelt anmodning er acceptabel.
28.	Systemet er udformet som et flerbrugersystem og på en sådan måde, at baggrundsopgaver fortsat kan udføres, mens brugeren udfører opgaver "i forgrunden".
29.	Systemet er udformet med henblik på løbende udvidelse, så det kan understøtte en potentiel forøgelse af antallet af meddelelser, når der tilføjes nye funktioner eller nye organisationer eller medlemsstater kommer til.

3.2.5 Sikkerhed

Nr.	Beskrivelse
30.	Systemet er egnet (f.eks. hvad angår sikkerhedsforanstaltninger) til udveksling af meddelelser med følsomme oplysninger af personlig karakter (f.eks. vedrørende ejere/brugere af køretøjer), der klassificeres som "EU Restricted".
31.	Systemet vedligeholdes på en sådan måde, at uautoriseret adgang til data hindres.
32.	Systemet indeholder en tjeneste, der behandler nationale slutbrugeres rettigheder og tilladelser.

Nr.	Beskrivelse
33.	Medlemsstaterne kan kontrollere afsenderens identitet (på medlemsstatsniveau), ved hjælp af en XML-signatur.
34.	Medlemsstaterne skal udtrykkelig give andre medlemsstater autorisation til at anmode om bestemte oplysninger.
35.	På programniveau omfatter systemet en komplet sikkerheds- og krypteringspolitik, der er i overensstemmelse med det sikkerhedsniveau, der kræves i sådanne tilfælde. Brug af XML-signatur og kryptering ved hjælp af SSL-tunneling sikrer, at oplysningerne ikke kommer ud, og garanterer deres integritet.
36.	Al udveksling af meddelelser kan spores ved hjælp af logføring.
37.	Der er beskyttelse mod sletningsangreb (en tredjepart sletter en meddelelse) og replay- eller indsætningsangreb (en tredjepart gensender eller indsætter en meddelelse).
38.	Systemet benytter certifikater fra en betroet tredjepart (TTP).
39.	Systemet kan håndtere forskellige certifikater for den enkelte medlemsstat, afhængig af meddelelsens eller tjenestens art.
40.	Sikkerhedsforanstaltningerne på programniveau er tilstrækkelige til at tillade brug af ikke-akkrediterede net.
41.	Systemet kan anvende ukomplicerede sikkerhedsteknikker såsom en XML-firewall.

3.2.6. Fleksibilitet

Nr.	Beskrivelse
42.	Systemet kan udbygges med nye meddelelser og nye funktioner. Tilpasningsomkostningerne er meget lave. Dette skyldes den centraliserede udvikling af programkomponenter.
43.	Medlemsstaterne kan definere nye meddelelsestyper til bilateral brug. Det er ikke nødvendigt, at alle medlemsstater understøtter alle meddelelsestyper.

3.2.7. Support og vedligeholdelse

Nr.	Beskrivelse
44.	Systemet omfatter overvågningsfaciliteter til brug for en central servicetjeneste og/eller centrale operatører for så vidt angår nettet og serverne i de forskellige medlemsstater.
45.	Systemet omfatter faciliteter til fjernsupport fra en central servicetjeneste.

Nr.	Beskrivelse
46.	Systemet omfatter faciliteter til problemanalyse.
47.	Systemet kan udbygges til nye medlemsstater.
48.	Programmet kan nemt installeres af personale med et minimum af færdigheder og erfaring inden for edb. Installationsproceduren skal automatiseres i størst muligt omfang.
49.	Systemet omfatter et miljø til brug for løbende testning og godkendelse.
50.	De årlige omkostninger til vedligeholdelse og support er reduceret mest muligt gennem overholdelse af markedsstandarderne og ved udformning af programmet, så der kræves mindst mulig support fra en central servicetjeneste.

3.2.8. Krav til udformingen

Nr.	Beskrivelse
51.	Systemet er udformet og forsynet med dokumentation med henblik på en lang driftslevetid.
52.	Systemet er udformet, så det er uafhængigt af netværksudbyderen.
53.	Systemet er foreneligt med medlemsstaternes nuværende hardware/software, idet det arbejder sammen med de registreringssystemer, der anvender åben standard-webtjenesteteknologi (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 osv.).

3.2.9. Standarder, der anvendes

Nr.	Beskrivelse
54.	Systemet er foreneligt med databeskyttelsesreglerne i forordning (EF) nr. 45/2001 (artikel 21, 22 og 23) og direktiv 95/46/EF.
55.	Systemet er foreneligt med IDA-standarderne.
56.	Systemet understøtter UTF-8.

Kapitel 4: Evaluering

1. Evalueringsprocedure i henhold til artikel 20 (Forberedelse af afgørelser omhandlet i artikel 25, stk. 2, i afgørelse 2008/.../RIA)

1.1. Spørgeskema

Den relevante arbejdsgruppe i Rådet udarbejder et spørgeskema vedrørende hver af de elektroniske dataudvekslinger, der er fastlagt i kapitel 2 i afgørelse 2008/.../RIA.

Så snart en medlemsstat mener, at den opfylder forudsætningerne for dataudveksling i den relevante datakategori, besvarer den det relevante spørgeskema.

1.2. Forsøgsfase

Med henblik på evaluering af resultaterne af spørgeskemaet gennemfører den medlemsstat, der ønsker at begynde at udveksle data, en forsøgsfase med en eller flere andre medlemsstater, der allerede udveksler data i medfør af Rådets afgørelse. Forsøgsfasen finder sted umiddelbart før eller efter evalueringsbesøget.

Vilkårene for og de nærmere bestemmelser om denne forsøgsfase identificeres af den relevante arbejdsgruppe i Rådet og baseres på forudgående aftale med den pågældende medlemsstat. De praktiske detaljer fastlægges af de medlemsstater, der deltager i forsøgsfasen.

1.3. Evalueringsbesøg

Med henblik på evaluering af resultaterne af spørgeskemaet gennemføres der et evalueringsbesøg i den medlemsstat, der ønsker at begynde at udveksle data.

Vilkårene for og de nærmere bestemmelser om besøget identificeres af den relevante arbejdsgruppe og baseres på forudgående aftale mellem den pågældende medlemsstat og evalueringsgruppen. Den pågældende medlemsstat giver evalueringsgruppen mulighed for at kontrollere den elektroniske dataudveksling i den eller de datakategorier, der skal evalueres, navnlig ved at tilrettelægge et program for besøget, som tager hensyn til evalueringsgruppens ønsker.

Inden en måned fremlægger evalueringsgruppen en rapport om evalueringsbesøget, som den sender til den pågældende medlemsstat med henblik på bemærkninger. Gruppen vil i givet fald revidere denne rapport på baggrund af medlemsstatens bemærkninger.

Evalueringsgruppen består af højst 3 eksperter, der udpeges af de medlemsstater, der deltager i den elektroniske dataudveksling i de datakategorier, der skal evalueres, og som har erfaringer med hensyn til den pågældende datakategori, relevant national sikkerhedsgodkendelse til at behandle disse spørgsmål og er rede til at deltage i mindst et evalueringsbesøg i en anden medlemsstat. Kommissionen vil blive indbudt til at deltage i evalueringsgruppen som observatør.

Medlemmerne af evalueringsgruppen respekterer den fortrolige karakter af de oplysninger, de kommer i besiddelse af, når de varetager deres opgave.

1.4. Rapport til Rådet

Rådet forelægges en samlet evalueringsrapport, som opsummerer resultaterne af spørgeskemaerne, evalueringsbesøget og forsøgsfasen, med henblik på Rådets afgørelse i henhold til artikel 25, stk. 2, i afgørelse 2008/.../RIA.

2. Evalueringsprocedure i henhold til artikel 21

2.1. Statistikker og rapport

Hver medlemsstat indsamlet statistikker om resultaterne af den elektroniske dataudveksling. For at sikre, at statistikkerne er sammenlignelige, vil den relevante arbejdsgruppe i Rådet udarbejde statistikmodellen.

Statistikkerne sendes hvert år til generalsekretariatet, der udarbejder en sammenfattende oversigt over det forgangne år, og til Kommissionen.

Medlemsstaterne vil desuden regelmæssigt, men højst én gang hvert år, blive anmodet om at forelægge yderligere oplysninger om den administrative, tekniske og finansielle gennemførelse af elektronisk dataudveksling, som er nødvendig for at analysere og forbedre processen. Der vil på grundlag af disse oplysninger blive udarbejdet en rapport til Rådet.

2.2. Revision

Inden for en rimelig frist undersøger Rådet den her beskrevne evalueringsmekanisme og reviderer den i givet fald.

3. Ekspertmøder

Eksperterne mødes regelmæssigt i den relevante arbejdsgruppe i Rådet med henblik på at tilrettelægge og gennemføre ovennævnte evalueringsprocedurer, udveksle erfaringer og drøfte mulige forbedringer. Resultaterne af disse ekspertdrøftelser vil eventuelt blive indarbejdet i den rapport, der nævnes i punkt 2.1.
