►B

DECISÃO 2008/616/JAI DO CONSELHO

de 23 de Junho de 2008

referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras

(JO L 210 de 6.8.2008, p. 12)

Alterada por:

		Jornal Oficial		
		n.º	página	data
►M1	Regulamento (UE) 2024/982 do Parlamento Europeu e do Conselho de 13 de março de 2024	L 982	1	5.4.2024

▼B

DECISÃO 2008/616/JAI DO CONSELHO

de 23 de Junho de 2008

referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras

CAPÍTULO 1

GENERALIDADES

Artigo 1.º

Objectivo

O objectivo da presente decisão é estabelecer as disposições administrativas e técnicas necessárias à execução da Decisão 2008/615/JAI, especialmente no que respeita ao intercâmbio automatizado de dados de ADN, dados dactiloscópicos e dados relativos ao registo de veículos, como previsto no capítulo 2 da referida decisão, e a outras formas de cooperação previstas no capítulo 5 da mesma.

Artigo 2.º

Definições

Para efeitos da presente decisão, entende-se por:

a) «Consulta» e «comparação», a que se referem os artigos 3.º, 4.º e 9.º da Decisão 2008/615/JAI, os procedimentos através dos quais se estabelece a existência de uma concordância entre, respectivamente, os dados de ADN ou os dados dactiloscópicos comunicados por um Estado-Membro e os dados de ADN ou os dados dactiloscópicos armazenados nas bases de dados de um, de vários ou de todos os Estados-Membros;

b) «Consulta automatizada», a que se refere o artigo 12.º da Decisão 2008/615/JAI, o procedimento de acesso em linha para consulta das bases de dados de um, de vários ou de todos os Estados-Membros;

c) «Perfil de ADN», um código alfanumérico que representa um conjunto de características de identificação da parte, não portadora de códigos, de uma amostra de ADN humano analisado, ou seja, a estrutura molecular específica presente nos diversos segmentos (*loci*) de ADN;

d) «Parte não portadora de códigos de ADN», as zonas de cromossomas sem expressão genética, ou seja, inaptas a fornecer quaisquer propriedades funcionais de um organismo;

e) «Dados de ADN de referência», um perfil de ADN e um índice de referência;

f) «Perfil de ADN de referência», o perfil de ADN de uma pessoa identificada;

g) «Perfil de ADN não identificado», o perfil de ADN obtido a partir de vestígios recolhidos durante a investigação de infracções penais e pertencentes a uma pessoa ainda por identificar;

▼B

h) «Anotação», a marca que um Estado-Membro acrescenta a um perfil de ADN na sua base de dados nacional indicando que esse perfil já foi objecto de concordância aquando de uma consulta ou comparação efectuada por outro Estado-Membro;

i) «Dados dactiloscópicos», impressões digitais, impressões digitais latentes, impressões palmares, impressões palmares latentes e modelos dessas impressões (codificação de pormenores), armazenados e tratados numa base de dados automatizada;

j) «Dados relativos ao registo de veículos», conjunto dos dados tal como especificado no capítulo 3 do anexo da presente decisão;

k) «Caso concreto», a que se referem a segunda frase do n.º 1 do artigo 3.º, a segunda frase do n.º 1 do artigo 9.º e o n.º 1 do artigo 12.º da Decisão 2008/615/JAI, designa uma única investigação ou um único procedimento penal. Se tal ficheiro contiver mais do que um perfil de ADN, dado dactiloscópico ou dado relativo ao registo de veículos, esses perfis ou dados podem ser transmitidos conjuntamente num único pedido de consulta.

▼M1

———————

▼B

CAPÍTULO 6

COOPERAÇÃO POLICIAL

Artigo 17.º

Patrulhas e outras intervenções conjuntas

1. Em conformidade com o capítulo 5 da Decisão 2008/615/JAI e, em particular, com as declarações apresentadas em aplicação do n.º 4 do artigo 17.º e dos n.os 2 e 4 do artigo 19.º da referida decisão, cada Estado-Membro designa um ou mais pontos de contacto a fim de dar aos outros Estados-Membros a possibilidade de se dirigirem às autoridades competentes e cada Estado-Membro pode especificar os procedimentos que aplica à organização de patrulhas e outras intervenções conjuntas e às iniciativas de outros Estados-Membros relativamente a essas intervenções, bem como outros aspectos práticos e modalidades operacionais a elas aplicáveis.

2. O Secretariado-Geral do Conselho elabora e actualiza a lista dos pontos de contacto e informa as autoridades competentes de todas as alterações nela introduzidas.

3. As autoridades competentes de cada Estado-Membro podem apresentar uma iniciativa com vista à organização de uma intervenção conjunta. Antes do início de uma intervenção específica, as autoridades competentes a que se refere o n.º 2 determinam, verbalmente ou por escrito, as disposições aplicáveis, que podem incluir as seguintes informações pormenorizadas:

a) As autoridades dos Estados-Membros competentes para a intervenção;

b) O objectivo específico da intervenção;

▼B

c) O Estado-Membro de acolhimento onde deve ser realizada a intervenção;

d) A zona geográfica do Estado-Membro de acolhimento onde deve ser realizada a intervenção;

e) O período abrangido pela intervenção;

f) A assistência específica a fornecer pelo(s) Estado(s)-Membro(s) de origem ao Estado-Membro de acolhimento, incluindo funcionários ou outros agentes da autoridade pública, elementos materiais e financeiros;

g) Os funcionários que participam na intervenção;

h) O funcionário responsável pela intervenção;

i) As atribuições dos funcionários e outros agentes do ou dos Estados-Membros de origem no Estado-Membro de acolhimento durante a intervenção;

j) As armas, as munições e o equipamento específicos que os funcionários do Estado-Membro de origem podem utilizar durante a intervenção, em conformidade com a Decisão 2008/615/JAI;

k) A logística em termos de transporte, alojamento e segurança;

l) A repartição dos custos da intervenção conjunta, se esta diferir da prevista na primeira frase do artigo 34.º da Decisão 2008/615/JAI;

m) Quaisquer outras informações eventualmente necessárias.

4. As declarações, os procedimentos e as designações a que se refere o presente artigo são reproduzidos no manual referido no n.º 2 do artigo 18.º.

CAPÍTULO 7

DISPOSIÇÕES FINAIS

▼M1

———————

▼B

Artigo 19.º

Autoridades independentes competentes em matéria da protecção de dados

Nos termos do n.º 2 do artigo 18.º da presente decisão, os Estados-Membros informam o Secretariado-Geral do Conselho sobre as autoridades independentes competentes em matéria de protecção de dados ou sobre as autoridades judiciárias a que se refere o n.º 5 do artigo 30.º da Decisão 2008/615/JAI.

▼M1

———————

▼B

Artigo 22.º

Relação com o Acordo de Execução do Tratado de Prüm

Aos Estados-Membros vinculados pelo Tratado de Prüm aplicam-se as disposições relevantes da presente decisão e do seu anexo, depois de plenamente transpostas, em vez das disposições correspondentes do Acordo de Execução do Tratado de Prüm. Todas as outras disposições do Acordo de Execução continuam a ser aplicáveis entre as partes contratantes no Tratado de Prüm.

▼B

Artigo 23.º

Execução

Os Estados-Membros devem tomar as medidas necessárias para dar cumprimento às disposições da presente decisão nos prazos referidos no n.º 1 do artigo 36.º da Decisão 2008/615/JAI.

Artigo 24.º

Aplicação

A presente decisão produz efeitos vinte dias após a sua publicação no *Jornal Oficial da União Europeia*.

▼B

ANEXO

ÍNDICE

▼B

▼B

CAPÍTULO 1: **Intercâmbio de dados de ADN**

1. ***Questões forenses relacionadas com o ADN, regras de concordância e algoritmos***

1.1. *Propriedades dos perfis de ADN*

O perfil de ADN pode incluir 24 pares de números que correspondem aos alelos de 24 loci, igualmente utilizados nos procedimentos da Interpol em matéria de ADN. As designações destes loci constam do seguinte quadro:

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

Os 7 loci sombreados na linha de cima correspondem ao actual conjunto normalizado europeu de loci (ESS) e ao conjunto normalizado de loci da Interpol (ISSOL).

Regras de inclusão:

Os perfis de ADN disponibilizados pelos Estados-Membros para efeitos de consulta ou comparação, bem como os perfis de ADN enviados para efeitos de consulta e comparação devem incluir pelo menos 6 loci plenamente designados ([1]), podendo conter loci suplementares ou espaços em branco em função da sua disponibilidade. Os perfis de ADN de referência devem conter pelo menos 6 dos 7 ESS de loci. A fim de aumentar o grau de exactidão das concordâncias, todos os alelos disponíveis devem ser armazenados na base de dados indexada de perfis de ADN para efeitos de busca e comparação. Os Estados-Membros devem implementar o mais rapidamente possível eventuais novos ESS de loci adoptados pela União Europeia.

Não são permitidos perfis mistos por forma a que os valores de alelos de cada locus consistam em apenas dois números que podem ser idênticos em caso de homozigotia em determinado locus.

Os jokers (*wildcards*) e as microvariantes devem ser abordados de acordo com as seguintes regras:

— Qualquer valor não numérico, com excepção da amelogenina, contido no perfil (por exemplo «o», «f», «r», «na», «nr» or «un») deve ser convertido automaticamente para exportação para um joker (*) e comparado com todos.

— Os valores numéricos «0», «1» ou «99» contidos no perfil devem ser convertidos automaticamente para exportação para um joker (*) e comparados com todos.

— Se para um locus forem facultados 3 alelos, o primeiro será aceite e os restantes 2 devem ser automaticamente convertidos para exportação para um joker (*) e comparados com todos.

— Se forem fornecidos valores joker para 1 ou 2 alelos, serão pesquisadas ambas as permutações do valor numérico dado para o locus (por exemplo, 12* pode corresponder a 12,14 ou 9,12).

([1]) «Plenamente designados» significa que está incluída.

▼B

— As microvariantes de pentanucleótidos (Penta D, Penta E & CD4) serão comparadas de acordo com o seguinte esquema:

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

— As microvariantes de tetranucleótidos (os restantes loci são tetranucleótidos) serão comparadas de acordo com o seguinte esquema:

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. *Regras de concordância*

A comparação de 2 perfis de ADN será efectuada com base nos loci para os quais exista um par de valores alélicos em ambos os perfis. Pelo menos 6 loci plenamente designados (sem amelogenina) devem corresponder nos dois perfis de ADN antes que seja dada uma resposta de acerto.

A concordância total (qualidade 1) é definida como a identidade de todos os valores de alelos dos loci comparados contidos nos perfis de ADN. A concordância quase total («near match») é definida como a concordância de todos menos um dos alelos comparados, contidos em 2 perfis de ADN (Qualidades 2, 3 e 4). As concordâncias quase totais apenas serão aceites se houver pelo menos uma concordância total de 6 loci plenamente designados, correspondentes nos 2 perfis de ADN comparados.

A causa de uma concordância quase total pode ser:

— Um erro de dactilografia na introdução de um dos perfis de ADN na consulta ou na base de dados de ADN;

— um erro de determinação ou designação de alelos durante o processo de geração do perfil de ADN.

1.3. *Regras de notificação*

Tanto as concordâncias totais como as quase totais e os «não acertos» serão notificados.

O relatório de concordância é enviado ao ponto de contacto nacional requerente e facultado ao ponto de contacto nacional requerido (a fim de que possa avaliar a natureza e o número de possíveis pedidos subsequentes relativos a outros dados pessoais disponíveis e outras informações relacionadas com o perfil de ADN que corresponde ao acerto de acordo com os artigos 5.º e 10.º da Decisão 2008/615/JAI do Conselho.

2. ***Tabela de códigos dos Estados-Membros***

De acordo com a Decisão 2008/615/JAI, será utilizado o código ISO 3166-1 alpha-2 para a criação de nomes de domínio e outros parâmetros de configuração requeridos nas aplicações de intercâmbio de dados de ADN em rede fechada no âmbito de Prüm.

Os códigos ISO 3166-1 alpha-2 são os seguintes códigos dos Estados-Membros com duas letras.

▼B

Nomes dos Estados-Membros	Código	Nomes dos Estados-Membros	Código
Bélgica	BE	Luxemburgo	LU
Bulgária	BG	Hungria	HU
República Checa	CZ	Malta	MT
Dinamarca	DK	Países Baixos	NL
Alemanha	DE	Áustria	AT
Estónia	EE	Polónia	PL
Grécia	EL	Portugal	PT
Espanha	ES	Roménia	RO
França	FR	Eslováquia	SK
Irlanda	IE	Eslovénia	SI
Itália	IT	Finlândia	FI
Chipre	CY	Suécia	SE
Letónia	LV	Reino Unido	UK
Lituânia	LT		

3. ***Análise funcional***

3.1. *Disponibilidade do sistema*

Os pedidos apresentados de acordo com o artigo 3.º da Decisão 2008/615/JAI devem dar entrada na base de dados em causa por ordem cronológica de chegada e as respostas devem chegar ao Estado-Membro requerente no espaço de 15 minutos a contar da entrada dos pedidos.

3.2. *Segundo passo*

Quando um Estado-Membro recebe uma notificação de concordância, cabe ao respectivo ponto de contacto nacional a responsabilidade pela comparação dos valores do perfil apresentado no pedido com os valores do ou dos perfis recebidos em resposta a fim de validar e controlar o valor de prova do perfil. Os pontos de contacto nacionais podem entrar em contacto directo para efeitos de validação.

Os procedimentos de auxílio judiciário começam após a validação de uma concordância existente entre dois perfis com base numa concordância total ou quase total apuradas durante o processo de consulta automatizado.

4. ***Documento de controlo da interface ADN***

4.1. *Introdução*

4.1.1. Objectivos

Este capítulo define os requisitos que regem o intercâmbio de informações sobre perfis de ADN entre os sistemas de bases de dados de ADN de todos os Estados-Membros. Os campos de cabeçalho são definidos especificamente para o intercâmbio de dados de ADN no contexto de Prüm, a parte relativa aos dados baseia-se na parte relativa aos dados dos perfis de ADN no esquema XML definido para a passarela para o intercâmbio de dados de ADN da Interpol.

Os dados são trocados por SMTP (protocolo de transferência de correio electrónico) e outras tecnologias de ponta, através de um relé central de transmissão de correio disponibilizado pelo fornecedor de serviços da rede. O ficheiro XML é transportado como corpo da mensagem de correio.

▼B

4.1.2. Âmbito de aplicação

O presente ICD define apenas o conteúdo da mensagem (*email*). Todos os tópicos específicos de rede e de correio são definidos de modo uniforme de modo a que o intercâmbio de dados de ADN possa ter uma base técnica comum.

Alguns pontos importantes:

— formato do título da mensagem por forma a permitir o tratamento automático das mensagens;

— necessidade ou não de cifrar o conteúdo e, em caso afirmativo, quais os métodos a escolher;

— comprimento máximo das mensagens.

4.1.3. Estrutura e princípios XML

A mensagem XML envolve duas partes:

— a parte do cabeçalho com informações sobre a transmissão e

— a parte dos dados com as informações específicas sobre o perfil, bem como o próprio perfil.

Deve ser utilizado o mesmo esquema XML quer se trate de pedidos, quer de respostas.

Para efeitos de controlos completos de perfis de ADN não identificados (artigo 4.º da Decisão 2008/615/JAI) deve ser possível enviar um lote de perfis numa só mensagem. Deve ser definido um número máximo de perfis numa só mensagem. O número depende da dimensão máxima permitida de mensagem e deve ser definido após a selecção do servidor de correio.

Exemplo de XML:

<?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>estrutura de dados repetida em caso de perfis múltiplos enviados numa mensagem (…) SMTP única, apenas permitida em caso de dados de acordo com o artigo 4.º]

</PRUEMDNA>

4.2. *Definição da estrutura XML*

As seguintes definições são apresentadas para efeitos de documentação e melhor legibilidade, a informação vinculativa real é fornecida num ficheiro em formato XML (PRUEM DNA.xsd).

▼B

4.2.1. Formato PRUEMDNAx

Contém os seguintes campos:

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

4.2.2. Conteúdo da estrutura do cabeçalho

4.2.2.1. Cabeçalho PRUEM

Esta estrutura descreve o cabeçalho do ficheiro XML e é composta pelos seguintes campos:

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

Tipo de dados constantes da mensagem, cujo valor pode ser:

Value	Description
R	Request
A	Answer

4.2.2.3. Cabeçalho PRUEM info

Estrutura para identificar o Estado-Membro, bem como a data/hora da mensagem. Contém os seguintes campos:

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. Conteúdo dos dados dos perfis PRUEM

4.2.3.1. Dados PRUEM

Esta estrutura descreve a parte dos dados de perfis em formato XML. Contém os seguintes campos:

▼B

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. Modelo de pedido PRUEM

Tipo de dados constantes da mensagem, cujo valor pode ser:

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

4.2.3.3. Tipo de qualidade do acerto PRUEM

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

▼B

4.2.3.4. Tipo de dados PRUEM

Tipo de dados contidos na mensagem, cujo valor pode ser:

Value	Description
P	Person profile
S	Stain

4.2.3.5. Resultados dos dados PRUEM

Tipo de dados contidos na mensagem, cujo valor pode ser:

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

4.2.3.6. Perfil de ADN IPSG

Esta estrutura descreve o perfil ADN. Contém os seguintes campos:

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

Estrutura com os loci do ISSOL (conjunto normalizado de loci da Interpol). Contém os seguintes campos:

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

▼B

Fields	Type	Description
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

Estrutura com os outros loci. Contém os seguintes campos:

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

Estrutura para descrever um locus. Contém os seguintes campos:

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

5. ***Arquitectura da aplicação, da segurança e da comunicação***

5.1. *Síntese*

Para efeitos de implementação de aplicações destinadas ao intercâmbio de dados de ADN no âmbito da Decisão 2008/615/JAI, deve ser utilizada uma rede comum de comunicação restrita aos Estados-Membros. A fim de aproveitar esta infra-estrutura de comunicação comum de

▼B

envio e recepção de pedidos e respostas de um modo mais eficaz, é adoptado um mecanismo assíncrono para transmitir pedidos de dados de ADN e dactiloscópicos em mensagens protegidas de correio electrónico SMPT. Para ir ao encontro de preocupações de segurança, será utilizado o mecanismo sMIME em extensão da funcionalidade SMPT a fim de estabelecer um verdadeiro túnel seguro de ponta a ponta através da rede.

A rede operacional TESTA (*Trans European Services for Telematics between Administrations* — Serviços telemáticos transeuropeus entre administrações) é utilizada como rede de comunicação para o intercâmbio de dados entre os Estados-Membros. A TESTA é gerida pela Comissão Europeia. Tendo em conta que as bases nacionais de ADN e os actuais pontos nacionais de acesso à rede TESTA podem encontrar-se em locais diferentes nos Estados-Membros, o acesso TESTA pode ser criado quer:

1) utilizando o ponto de acesso nacional existente ou estabelecendo um novo ponto de acesso nacional à TESTA; quer

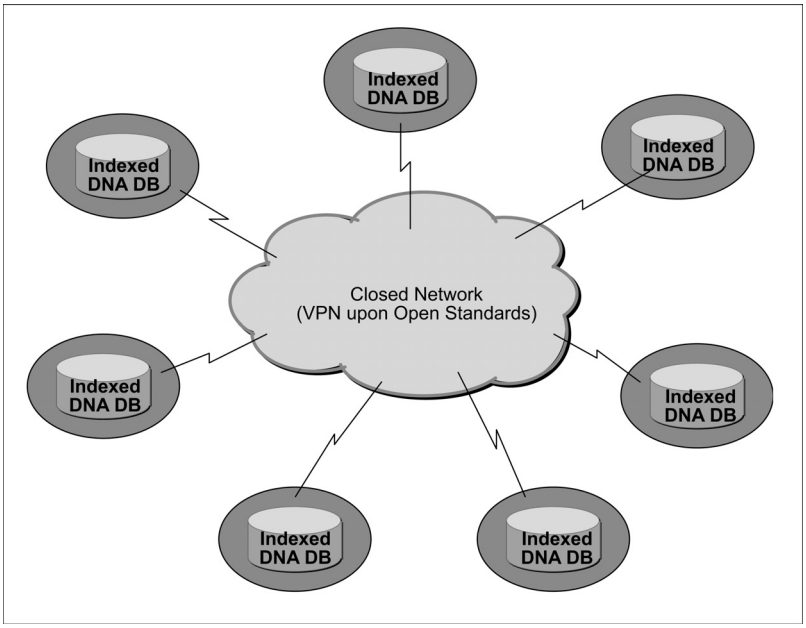
2) estabelecendo uma ligação local segura entre o local onde se encontra e é gerida pelo serviço nacional competente a base de dados de ADN e o ponto de acesso nacional à TESTA.

Os protocolos e as normas utilizadas na implementação das aplicações decorrentes da Decisão 2008/615/JAI obedecem às normas abertas e cumprem os requisitos impostos pelos decisores políticos dos Estados-Membros em matéria de segurança.

5.2. *Arquitectura de nível superior*

No âmbito da Decisão 2008/615/JAI, cada Estado-Membro disponibilizará os seus dados de ADN para efeitos de intercâmbio e/ou de consulta por outros Estados-Membros em conformidade com o formato de dados normalizado comum. A arquitectura baseia-se num modelo de comunicação de qualquer a qualquer (*any-to-any*). Não há nenhum servidor central nem nenhuma base de dados centralizada para armazenar perfis de ADN.

Figura 1: Topologia do intercâmbio de dados de ADN



▼B

Sob reserva dos requisitos legais nacionais nos locais dos Estados-Membros, cada Estado-Membro pode determinar o tipo de equipamento e *software* que deve ser utilizado para que a configuração do seu sítio obedeça aos requisitos constantes da Decisão 2008/615/JAI.

5.3. *Normas de segurança e protecção de dados*

Foram analisados e implementados três níveis de segurança.

5.3.1. Nível de dados

Os dados de perfis de ADN transmitidos por cada Estado-Membro devem obedecer a uma norma comum de protecção de dados por forma a que os Estados-Membros requerentes recebam uma resposta que indique sobretudo se há acerto ou não (HIT NO-HIT), junto com um número de identificação em caso de acerto, mas que não deve conter nenhuma informação de carácter pessoal. A investigação subsequente à notificação de um acerto será conduzida a nível bilateral de acordo com a regulamentação jurídica e administrativa dos sítios dos Estados-Membros.

5.3.2. Nível de comunicação

As mensagens que contêm informação (requerente e de resposta) sobre perfis de ADN serão cifradas por um sistema de ponta compatível com as normas abertas, como as sMIME antes de serem enviadas para os sítios de outros Estados-Membros.

5.3.3. Nível de transmissão

Todas as mensagens cifradas com informações relativas a perfis de ADN serão transmitidas para sítios de outros Estados-Membros através de um sistema de tunelização privado administrado por um fornecedor de rede reconhecido a nível internacional e de ligações securizadas a este sistema sob responsabilidade nacional. Este sistema virtual de tunelização privado não tem nenhuma ligação à internet aberta.

5.4. *Protocolos e normas a utilizar para o mecanismo de cifragem: sMIME e pacotes conexos*

A norma aberta sMIME enquanto extensão da norma de correio electrónico SMTP será utilizada para cifrar mensagens com informações relativas a perfis de ADN. O protocolo sMIME (V3) permite dispor de recibos assinados, rótulos de segurança e listas de endereços e baseia-se na sintaxe de mensagens criptográficas (CMS), uma especificação IETF para as mensagens protegidas por cifragem. Pode igualmente ser utilizada para assinatura, conversão, autenticação ou cifragem electrónicas de qualquer forma de dados digitais.

O certificado subjacente utilizado pelo mecanismo sMIME deve obedecer à norma X.509. A fim de assegurar normas e procedimentos comuns a outras aplicações Prüm, as regras de tratamento para operações de cifragem sMIME ou que devam ser aplicados em diferentes ambientes COTS (disponíveis no comércio) são as seguintes:

— A sequência das operações é a seguinte: primeiro cifragem e depois assinatura;

— Para a cifragem simétrica e assimétrica, serão aplicados, respectivamente, os algoritmos criptográficos AES (Norma Avançada de Cifragem — *Advanced Encryption Standard*), com um comprimento de código de 256 bits, e RSA, com um comprimento de código de 1 024 bits;

— Será aplicado o algoritmo de sumário SHA-1.

▼B

A funcionalidade sMIME está integrada na grande maioria dos pacotes de *software* modernos de correio electrónico, nomeadamente Outlook, Mozilla Mail e Netscape Communicator 4.x e é compatível com todos os principais pacotes de *software* de correio electrónico.

Dada a sua fácil integração na infra-estrutura nacional TI de todos os sítios dos Estados-Membros, o sMIME foi seleccionado como mecanismo viável para a implementação do nível de segurança das comunicações. Todavia, a fim de alcançar o objectivo de «validação de conceito» de uma forma mais eficaz e de reduzir os custos, opta-se pela norma aberta API JavaMail para o protótipo do intercâmbio de dados de ADN. A API JavaMail permite a cifragem e a decifragem simples de mensagens de correio electrónico que utilizem s/MIME e/ou OpenPGP. O objectivo é de dispor de uma API única de fácil utilização para os clientes de correio electrónico que pretendam enviar e receber mensagens cifradas num dos dois formatos de cifragem de correio electrónico mais correntes. Por conseguinte, para satisfazer os requisitos da Decisão 2008/615/JAI, bastará qualquer aplicação avançada para o API JavaMail, como o Bouncy Castle JCE (*Java Cryptographic Extension* — extensão criptográfica JAVA), que será utilizada para implementar o sMIME como protótipo para o intercâmbio de dados de ADN entre todos os Estados-Membros.

5.5. *Arquitectura da aplicação*

Cada Estado-Membro fornecerá aos restantes Estados-Membros um conjunto de dados normalizados de perfis de ADN em conformidade com o actual ICD comum quer mediante um esquema lógico de cada base de dados nacional, quer criando uma base de dados física exportada (base de dados indexada).

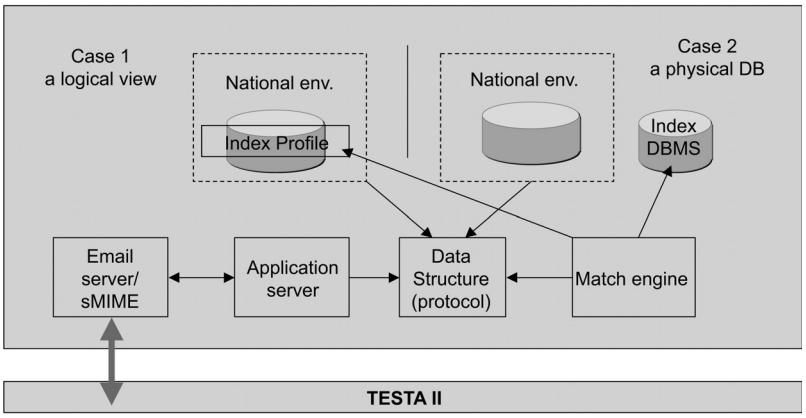
Os quatro principais componentes: servidor de correio electrónico/ /sMIME, servidor de aplicação, zona de estrutura de dados para extracção/alimentação de dados e registo de entrada/saída de mensagens, e o motor de concordância aplicam toda a lógica de aplicação de uma forma independente do produto.

A fim de que todos os Estados-Membros possam integrar facilmente os componentes nos seus sítios nacionais, a funcionalidade comum especificada foi implementada através de componentes abertos que podem ser seleccionados por cada Estado-Membro em função da sua política e regulamentação nacionais em matéria de TI. Cada Estado-Membro pode escolher livremente o equipamento e a plataforma de *software*, incluindo a base de dados e os sistemas operativos, tendo em conta as características independentes a implementar para obter o acesso às bases de dados indexadas que contêm perfis de ADN abrangidas pela Decisão 2008/615/JAI.

Foi desenvolvido e testado com êxito na rede comum existente um protótipo para o intercâmbio de dados de ADN. A versão 1.0 foi introduzida no ambiente de produção e está ser utilizada nas operações correntes. Os Estados-Membros podem utilizar o produto que foi desenvolvido em conjunto, mas também podem desenvolver os seus próprios produtos. Os componentes do produto comum serão mantidos, adaptados e desenvolvidos no futuro em função das alterações dos requisitos TI, forenses e/ou de política funcional.

▼B

Figura 2: Diagrama da topologia da aplicação



5.6. *Protocolos e normas a utilizar na arquitectura da aplicação:*

5.6.1. XML

O intercâmbio de dados de ADN aproveitará plenamente o esquema XML na forma de anexo às mensagens de correio electrónico SMTP. A XML (*eXtensible Markup Language* — Linguagem de Marcação Expansível) é uma linguagem de marcação de uso geral recomendada pelo W3C (World Wide Web Consortium — Consórcio da Web) para a criação de linguagens de marcação especializadas, capaz de descrever muitos tipos diferentes de dados. A descrição do perfil de ADN que se presta ao intercâmbio entre todos os Estados-Membros foi efectuada com a XML e o esquema XML no documento ICD.

5.6.2. ODBC

A conectividade de bases de dados abertas (*Open DataBase Connectivity*) constitui um método normalizado de software API para aceder a sistemas de gestão de bases de dados que a torna independente das linguagens de programação, bases de dados e sistemas operativos. A ODBC tem contudo de algumas limitações: a administração de um grande número de máquinas-cliente pode implicar uma grande diversidade de pilotos e DLLs. Esta complexidade pode dificultar a administração do sistema.

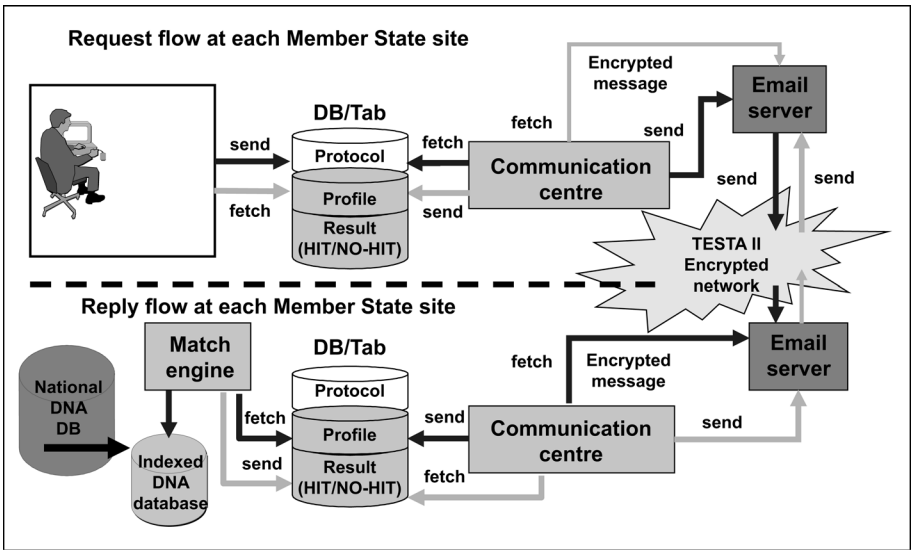
5.6.3. JDBC

A conectividade de bases de dados Java (JDBC — *Java DataBase Connectivity*) é uma interface API da linguagem de programação Java que determina a forma como um cliente pode aceder a uma base de dados. Ao contrário da ODBC, a JDBC não requer a utilização de um certo conjunto de DLLs locais no sistema de secretária (desktop).

O diagrama seguinte descreve a lógica funcional do tratamento dos pedidos e respostas de perfis de ADN no sítio de cada Estado-Membro. Os fluxos dos pedidos e respostas interagem com a zona de dados neutra que comporta diferentes conjuntos de dados, com uma estrutura de dados comuns.

▼B

Figura 3: Diagrama do fluxo de dados da aplicação no sítio de cada Estado-Membro



5.7. *Ambiente de comunicação*

5.7.1. Rede comum de comunicações: TESTA e sua infra-estrutura de apoio

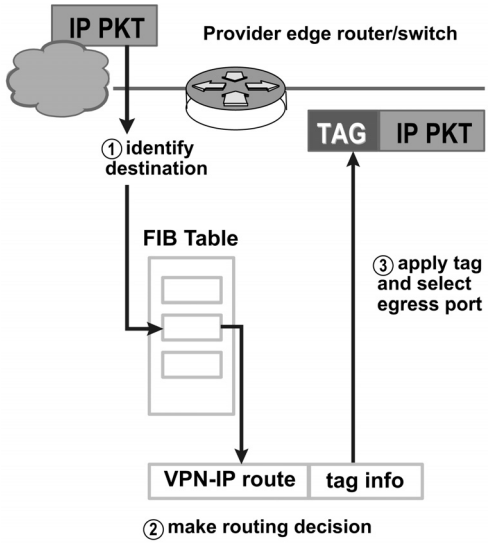
A aplicação destinada ao intercâmbio de dados de ADN aproveitará o correio electrónico, um mecanismo assíncrono, para o envio e recepção de pedidos e respostas entre Estados-Membros. Dado que todos os Estados-Membros dispõem de pelo menos um ponto nacional de acesso à rede TESTA, o intercâmbio dos dados de ADN processar-se-á através desta rede. A TESTA oferece uma série de serviços de valor acrescentado graças ao seu relé de correio electrónico. Para além de acolher caixas de correio específicas da TESTA, a infra-estrutura possibilita listas de distribuição de correio e opções de encaminhamento. Deste modo, a TESTA pode ser utilizada como central de compensação para mensagens dirigidas às administrações ligadas a domínios União Europeia. Também podem ser instalados programas antivírus.

O relé de correio TESTA está integrado numa plataforma *hardware* de alta disponibilidade nas instalações centrais da aplicação TESTA e é protegido por corta-fogo. Os serviços de nomes de domínio (DNS) da TESTA converterão os localizadores de recursos em endereços IP e ocultarão os elementos de endereço aos utilizadores e às aplicações.

5.7.2. Preocupações de segurança

O conceito de VPN (rede privada virtual) foi aplicado no âmbito da TESTA. A tecnologia utilizada para criar esta VPN será adaptada para poder suportar a norma MPLS (*Multi-Protocol Label Switching*) desenvolvida pelo Grupo de Missão de Engenharia da Internet (IETF).

▼B



A MPLS é uma norma IETF que acelera o fluxo de tráfico na rede ao evitar a análise de pacote pelos encaminhadores intermédios (hops). Isso é feito com base nas chamadas etiquetas que são apensas ao pacote pelos encaminhadores charneira da espinha dorsal (*backbone*), a partir da informação armazenada na base de informação que envia a informação (*forwarding information base* — FIB). As etiquetas são igualmente utilizadas para implementar redes privadas virtuais (VPN).

A MPLS associa as vantagens do encaminhamento da camada 3 às vantagens da comutação da camada 2. Dado que os endereços IP não são avaliados durante a transição na espinha dorsal, a MPLS não impõe nenhumas limitações de endereço IP.

Além disso, as mensagens de correio electrónico via TESTA serão protegidas pelo mecanismo de cifragem da sMIME. Sem conhecer a chave e possuir o devido certificado, ninguém pode decifrar as mensagens que circulam na rede.

5.7.3. Protocolos e normas a utilizar na rede de comunicações

5.7.3.1. SMTP

O protocolo de transferência de correio electrónico (*Simple Mail Transfer Protocol)* é a norma de facto para a transmissão de correio electrónico na internet. O SMPT é um protocolo textual relativamente simples, em que são especificados um ou mais destinatários da mensagem, sendo depois enviado o texto da mensagem. O SMTP utiliza a porta TCP 25 conforme especificado pelo IETF. Para determinar o servidor SMPT para um dado nome de domínio, utiliza-se o registo MX (*Mail Exchange* – troca de correio electrónico) DNS (sistema de nomes de domínio).

Uma vez que este protocolo se baseia exclusivamente em caracteres ASCII, era dificilmente compatível com ficheiros binários. Foram desenvolvidas normas como a norma MIME para codificar ficheiros binários com vista à sua transferência através do SMTP. Hoje em dia, a maior parte dos servidores SMTP aceita a extensão 8BITMIME e sMIME, o que permite o envio de ficheiros binários quase tão facilmente como o simples texto. As regras de tratamento das operações sMIME são descritas na secção dedicada a esta norma (ver capítulo 5.4).

O SMPT é um protocolo de extracção (push) que não permite extrair mensagens a partir de um servidor remoto a pedido. Para o efeito, o cliente de correio electrónico deve utilizar o POP3 ou o IMAP. No âmbito da implementação do intercâmbio de dados de ADN, foi decidido utilizar o protocolo POP3.

▼B

5.7.3.2. POP

Os clientes locais de correio electrónico utilizam a versão 3 do protocolo (POP3), um protocolo internet normalizado de aplicação em camada, para extrair mensagens de correio electrónico de um servidor remoto através de uma conexão TCP/IP. Ao usar o perfil SMTP Submit do protocolo SMTP, os clientes de correio electrónico enviam mensagens através da internet ou através de uma rede empresarial. A norma MIME é utilizada nos anexos e no texto não ASCII no correio electrónico. Embora nem o POP3 nem o SMPT requeiram mensagens electrónicas em formato MIME, praticamente todas as mensagens internet chegam em formato MIME, pelo que os clientes POP devem aceitar e utilizar essa norma. Todo o ambiente de comunicação da Decisão 2008/615/JAI incluirá por conseguinte os componentes POP.

5.7.4. Atribuição de endereços de rede

Ambiente operativo

Actualmente, a autoridade de registo IP europeia (RIPE) reservou um bloco específico da sub-rede da classe C à TESTA. De futuro, poderão ser atribuídos novos blocos de endereços à TESTA, se tal for necessário. A atribuição de endereços IP aos Estados-Membros baseia-se num esquema geográfico europeu. O intercâmbio de dados entre Estados-Membros no âmbito da Decisão 2008/615/JAI processa-se através de uma rede IP europeia logicamente fechada.

Ambiente de ensaio

A fim de providenciar as condições necessárias ao bom funcionamento quotidiano entre todos os Estados-Membros ligados, deve ser criado um ambiente de ensaio da rede fechada para novos Estados-Membros que estejam a preparar-se para participar nas operações. Foi definida uma ficha de parâmetros, incluindo endereços IP, parâmetros de rede, domínios de correio electrónico, bem como contas de utilizadores, que deve ser implementada no sítio do Estado-Membro correspondente. Além disso, foi criado um conjunto de perfis de ADN fictícios para efeitos de ensaio.

5.7.5. Parâmetros de configuração

É criado um sistema seguro de correio electrónico que utiliza o domínio eu-admin.net. Este domínio, bem como os endereços que lhe estão associados não será acessível a partir de uma localização não pertencente ao domínio europeu TESTA, visto que os nomes apenas são conhecidos do servidor DNS central da TESTA que se encontra protegido da internet.

O mapeamento destes endereços de sítios TESTA (nomes internet) para os respectivos endereços IP é efectuado pelo serviço DNS da TESTA. Para cada Domínio Local, será inserida uma entrada Correio neste servidor DNS central da TESTA, o que faz com que todas as mensagens de correio enviadas aos Domínios Locais TESTA sejam retransmitidas ao Relé de Correio central TESTA. Este Relé de Correio central TESTA reenvia depois as mesmas ao servidor de correio específico do Domínio Local, utilizando os endereços do Domínio Local. Ao encaminhar as mensagens desta forma, as informações críticas nelas contidas apenas passarão pela infra-estrutura fechada europeia e não pela internet insegura.

▼B

É necessário estabelecer subdomínios (***a negro e em itálico***) em todos os sítios de todos os Estados-Membros que obedecem à seguinte sintaxe:

«tipo de aplicação.**pruem.*código do Estado-Membro.***eu-admin.net», onde

«código do Estado-Membro» corresponde ao código de duas letras do Estado-Membro (p.ex. AT, BE, etc.).

«***tipo de aplicação***» corresponde a: ADN e FP.

Aplicando a sintaxe acima descrita, os subdomínios de cada Estado-Membro são enumerados no seguinte quadro:

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

▼B

MS	Sub Domains	Comments
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	

▼B

CAPÍTULO 2: **Intercâmbio de dados dactiloscópicos (documento de controlo de interface)**

O objectivo do documento de controlo de interface que se segue consiste em definir os requisitos para o intercâmbio de informação dactiloscópica entre os Sistemas Automáticos de Identificação Dactiloscópica (AFIS) dos Estados-Membros. Baseia-se na implementação pela Interpol da ANSI/NIST--ITL 1-2000 (INT-I, Versão 4.22b).

Esta versão abrangerá todas as definições básicas dos registos lógicos de tipo-1, tipo-2, tipo-4, tipo-9, tipo-13 e tipo-15 necessários para o tratamento dactiloscópico de imagens e minúcias.

1. ***Síntese do conteúdo do ficheiro***

Um ficheiro dactiloscópico consiste em vários registos lógicos. Existem dezasseis tipos de registos especificados na norma ANSI/ /NIST-ITL 1-2000 original. Entre cada registo e os campos e subcampos no interior dos registos são utilizados caracteres de separação ASCII adequados.

São utilizados apenas 6 tipos de registos para o intercâmbio entre os organismos de origem e de destino:

Tipo-1	→	Informação sobre a transacção
Tipo-2	→	Dados alfanuméricos relativos a pessoas/casos
Tipo-4	→	Imagens dactiloscópicas de elevada resolução em escala de cinzentos
Tipo-9	→	Registo de minúcias
Tipo-13	→	Registo de imagens latentes de resolução variável
Tipo-15	→	Registo de imagens palmares de resolução variável

1.1. *Tipo-1 — Cabeçalho do ficheiro*

Este registo contém informações de encaminhamento e informações descritivas da estrutura do restante ficheiro. Este tipo de registo define também os tipos de transacção que integram as seguintes grandes categorias:

1.2. *Tipo-2 — Texto descritivo*

Este registo contém texto com interesse para os organismos de envio e recepção.

1.3. *Tipo-4 — Imagem em escala de cinzentos de elevada resolução*

Este registo é utilizado para o intercâmbio de imagens dactiloscópicas de alta resolução em escala de cinzentos (8 bits) captadas a 500 píxeis/polegada. As imagens dactiloscópicas serão comprimidas usando o algoritmo WSQ com um rácio máximo de compressão de 15:1. Não podem ser utilizados outros algoritmos de compressão nem imagens não comprimidas.

1.4. *Tipo-9 — Registo de minúcias*

Os registos do tipo-9 são utilizados para trocar características das cristas ou minúcias. Destinam-se, por um lado, a evitar duplicações desnecessárias de processos de codificação AFIS e, por outro lado, a permitir a transmissão de códigos AFIS que contêm menos dados do que as imagens correspondentes.

▼B

1.5. *Tipo-13 — Registo de imagens latentes de resolução variável*

Este registo deve ser utilizado para o intercâmbio de imagens latentes de impressões digitais e palmares de resolução variável, juntamente com informações textuais alfanuméricas. A resolução das imagens deve ser de 500 píxeis/polegada com 256 tonalidades de cinzento. Se a qualidade da imagem latente for suficiente, deve ser comprimida utilizando o algoritmo WSQ. Se necessário, a resolução das imagens pode ser aumentada para mais de 500 píxeis/polegada e mais de 256 tonalidades de cinzento mediante acordo bilateral. Nesse caso, recomenda-se vivamente a utilização da norma JPEG 2000 (ver apêndice 7).

1.6. *Registo de imagens palmares de resolução variável*

Os registos de imagens em campo etiquetado do tipo-15 devem ser utilizados para o intercâmbio de imagens palmares de resolução variável, juntamente com informações textuais alfanuméricas. A resolução das imagens deve ser de 500 píxeis/polegada com 256 tonalidades de cinzento. Para minimizar o volume de dados, todas as imagens palmares devem ser comprimidas utilizando o algoritmo WSQ. Se necessário, a resolução das imagens pode ser aumentada para mais de 500 píxeis/polegada e mais de 256 tonalidades de cinzento mediante acordo bilateral. Nesse caso, recomenda-se vivamente a utilização da norma JPEG 2000 (ver apêndice 7).

2. ***Formato dos registos***

Um ficheiro de transacção consistirá em um ou mais registos lógicos. Para cada registo lógico contido no ficheiro, devem existir vários campos de informação adequados. Cada campo de informação pode incluir um ou mais elementos básicos de informação com um só valor. Agrupados estes elementos são utilizados para transmitir diferentes aspectos dos dados incluídos nesse campo. Os campos de informação podem igualmente incluir um ou mais elementos de informação agrupados e repetidas várias vezes no interior de um campo. Este grupo de elementos de informação é conhecido como subcampo. Os campos de informação podem, portanto, incluir um ou mais subcampos de elementos de informação.

2.1. *Separadores de informação*

Nos registos lógicos com campos etiquetados, a informação é delimitada mediante o uso de quatro separadores de informação ASCII. A informação delimitada pode consistir em elementos no interior de um campo ou subcampo, campos no interior de um registo lógico ou múltiplas ocorrências de subcampos. Estes separadores de informação são definidos na norma ANSI X3.4. Estes caracteres são utilizados para separar e qualificar a informação de um modo lógico. Numa relação hierárquica, o carácter «FS» (separador de ficheiro) é o mais abrangente, seguido pelo separador de grupo «GS», o separador de registos «RS» e, por último, os caracteres de separação de unidades «US». O quadro 1 lista estes separadores ASCII e descreve o seu uso no âmbito desta norma.

Os separadores de informação devem ser encarados do ponto de vista funcional como uma indicação do tipo de dados que se segue. O caracter «US» deve separar elementos individuais de informação no interior de um campo ou subcampo. Assinala-se deste modo que o elemento de informação que se segue pertence a este campo ou subcampo. Os subcampos múltiplos no interior de um campo separados pelo caracter «RS» indicam o início do novo grupo de elementos de informação repetidos. O separador «GS» entre campos de informação indica o início de um novo campo que precede o número de identificação do campo que se segue. Do mesmo modo, o início de um novo registo lógico será assinalado pela ocorrência do separador «FS».

▼B

Os quatro caracteres apenas têm significado como separadores de elementos de dados nos campos de registo de texto ASCII. Estes caracteres não possuem qualquer significado específico quando surgem em registos de imagens e campos binários, sendo apenas parte dos dados trocados.

Regra geral, não deverá haver campos ou elementos de informação vazios, pelo que deverá surgir apenas um caracter de separação entre dois elementos de dados. Existe uma excepção a essa regra quando os dados nos campos ou elementos de informação numa transacção não estiverem disponíveis, faltem ou sejam facultativos e o tratamento da transacção não depender da presença destes dados específicos. Nesses casos, surgirão caracteres de separação múltiplos e adjacentes, não sendo necessário inserir dados fictícios entre eles.

Para efeitos de definição de um campo composto por três elementos de informação, aplica-se o seguinte: se faltar o segundo elemento de informação, ocorrem dois separadores «US» adjacentes entre o primeiro e o terceiro elemento de informação. Se faltarem tanto o segundo como o terceiro elemento de informação, deverão ser usados três separadores — dois separadores «US» mais o separador que encerra o campo ou subcampo. Em suma, se faltarem num campo ou subcampo um ou mais elementos de informação obrigatórios ou facultativos, deverão ser inseridos separadores tantas vezes quanto apropriado.

Por conseguinte, é possível que se sucedam combinações de dois ou mais dos quatro separadores disponíveis. Quando faltam ou não estão disponíveis dados para certos elementos de informação, subcampos ou campos, terá de haver um separador a menos que o total exigido de elementos de informação, subcampos ou campos.

Quadro 1: Separadores utilizados

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. *Formato de registo*

No que respeita aos registos lógicos em campos etiquetados, cada campo de informação utilizado deve ser numerado de acordo com esta norma. Cada campo será formatado com o número de tipo de registo lógico, seguido de um ponto «.», um número de campo seguido de dois pontos «:», seguido da informação apropriada a esse campo. O número do campo etiquetado pode ser qualquer algarismo de 0 a 9 entre o ponto «.» e os dois pontos «:» e será interpretado como um número de campo inteiro não sinalizado. Isto significa que um número de campo «2.123» equivale e é interpretado do mesmo modo que um número de campo «2.000000123:».

Para efeitos de ilustração no presente documento, será utilizado um número de três algarismos para enumerar os campos constantes de cada registo lógico descrito. Os números de campo terão o formato «TT.xxx:», sendo «TT» o tipo de registo de um ou dois caracteres seguido de um ponto. Os três caracteres seguintes constituem o número de campo adequado seguido de dois pontos, seguidos de informação descritiva ASCII ou dos dados relativos à imagem.

▼B

Os registos lógicos do tipo-1 e do tipo-2 contêm apenas campos de dados com texto ASCII. O comprimento total do registo (incluindo números de campo, dois pontos e caracteres de separação) será inscrito como primeiro campo ASCII em cada um destes tipos de registos. Os caracteres «FS» do separador de ficheiro ASCII (que representam o fim do registo lógico ou transacção) vêm a seguir ao último byte de informação ASCII e são incluídos no comprimento do registo.

Ao contrário do conceito de campo etiquetado, o registo de tipo-4 apenas contém dados binários registados como campos binários ordenados de comprimento fixo. Todo o comprimento do registo será inscrito no primeiro campo binário de quatro bytes de cada registo. Neste registo binário, não serão inscritos nem o número de registo com o seu ponto nem o número identificador de campo com os seus dois pontos. Além disso, uma vez que todos os comprimentos de campo deste registo são fixados ou especificados, os quatro separadores («US», «RS», «GS», ou «FS») só podem ser interpretados como sendo dados binários. No registo binário, o caracter «FS» não será utilizado como separador nem como carácter de fim de transacção.

3. ***Registo lógico de tipo 1: cabeçalho do ficheiro***

Este registo descreve a estrutura e o tipo do ficheiro, bem como outras informações importantes. O conjunto de caracteres utilizado para campos do tipo-1 apenas contém o código ANSI de 7 bits para o intercâmbio de informações.

3.1. *Campos para o registo lógico de tipo-1*

3.1.1. Campo 1.001: comprimento de registo lógico (LEN — *Logical Record Length*)

Este campo contém o número total de bytes em todo o registo lógico do tipo-1. O campo começa com «1.001:» seguido do comprimento total do registo incluindo todos os caracteres de todos os campos e os separadores de informação.

3.1.2. Campo 1.001: número de versão (VER)

Para assegurar que os utilizadores conheçam a versão da norma ANSI/NIST que está a ser utilizada, este campo de quatro bytes especifica o número da versão da norma que está a ser aplicada pelo *software* ou pelo sistema de cria o ficheiro. Os dois primeiros bytes especificam o número de referência da versão principal e os dois segundos, o número de revisão menor. Por exemplo, a norma original de 1986 será considerada a primeira versão e designada por «0100» ao passo que a actual norma ANSI/NIST-ITL 1-2000 tem a designação de «0300».

3.1.3. Campo 1.003: conteúdo do ficheiro (CNT)

Este campo enumera cada um dos registos no ficheiro de acordo com o tipo e a ordem pela qual os registos aparecem no ficheiro lógico. Consistem em um ou mais subcampos que contêm dois elementos de informação descritivos de um registo lógico único encontrado no ficheiro. Os subcampos são introduzidos pela ordem em que os registos são introduzidos e transmitidos.

O primeiro elemento de informação no primeiro subcampo é o «1» e identifica o registo do tipo-1. Segue-se um segundo elemento de informação que contém o número de outros registos incluídos no ficheiro. Este número corresponde ao número de subcampos restantes do campo 1.003.

▼B

Cada um dos subcampos restantes está associado a um registo no ficheiro e a sequência de subcampos corresponde à sequência dos registos. Cada subcampo contém dois elementos de informação: o primeiro identifica o tipo de registo; o segundo corresponde ao IDC do registo. O caracter «US» deve ser utilizado para separar os dois elementos de informação.

3.1.4. Campo 1.004: tipo de transacção (TOT)

Este campo contém uma mnemónica que designa o tipo de transacção. Estes códigos podem ser diferentes dos utilizados por outras aplicações da norma ANSI/NIST.

CPS: busca de impressão em contexto penal (CPS — *Criminal Print-to-Print Search*). Esta transacção é um pedido de pesquisa numa base de dados de impressões digitais de um registo relacionado com uma infracção penal. As impressões digitais da pessoa devem ser incluídas no ficheiro como imagens WSQ comprimidas.

Em caso de não acerto (No-Hit), serão devolvidos os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

Em caso de acerto (HIT), serão devolvidos os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

— 1-14 registos de tipo-4

Consta do Quadro A.6.1 (Apêndice 6) um resumo do TOT CPS.

PMS: pesquisa impressão digital-latente. Recorre-se a esta transacção quando um conjunto de impressões digitais é comparado com uma base de dados de Latentes Não Identificadas. A resposta conterá o resultado Acerto/Não acerto da busca do AFIS de destino. Caso existam latentes não identificados múltiplos, serão devolvidas transacções SER múltiplas, cada uma com uma imagem latente. As impressões digitais da pessoa devem ser incluídas no ficheiro como imagens WSQ comprimidas.

Em caso de não acerto, a resposta incluirá os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

Em caso de acerto, a resposta incluirá os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

— 1 registo de tipo-13

Consta do Quadro A.6.1 (Apêndice 6) um resumo do TOT PMS.

MPS: pesquisa imagem latente — impressões digitais. Esta transacção é utilizada para comparar uma imagem latente com as impressões digitais contidas numa base de dados. Os pormenores da imagem latente e a imagem (comprimida com o algoritmo WSQ) devem ser incluídos no ficheiro.

Em caso de não acerto, a resposta incluirá os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

▼B

Em caso de acerto, a resposta incluirá os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

— 1 registo do tipo-4 ou do tipo-15

Consta do Quadro A.6.4 (Apêndice 6) um resumo do TOT MSP.

MMS: pesquisa imagem latente — imagem latente. Nesta transacção, o ficheiro contém uma imagem latente que deve ser conferida com uma base de dados de imagens latentes não identificadas a fim de estabelecer relações entre os vários locais do crime. Os pormenores da imagem latente e a imagem (comprimida com o algoritmo WSQ) devem ser incluídas no ficheiro.

Em caso de não acerto, a resposta incluirá os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

Em caso de acerto, a resposta incluirá os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

— 1 registo de tipo-13

Consta do Quadro A.6.4 (Apêndice 6) um resumo do TOT MMS.

SRE: esta transacção constitui a resposta do serviço de destino a pedidos com dados dactiloscópicos. A resposta incluirá o resultado acerto/não acerto da pesquisa AFIS na base de dados de destino. Caso existam candidatos múltiplos, serão devolvidas transacções SRE múltiplas, cada uma com um candidato.

Consta do Quadro A.6.2 (Apêndice 6) um resumo do TOT SRE.

ERR: esta transacção constitui a resposta do AFIS de destino para assinalar erros na transacção. Inclui um campo (ERM) para indicar o erro que foi detectado. Serão enviados os seguintes registos lógicos:

— 1 registo de tipo-1

— 1 registo de tipo-2

Consta do Quadro A.6.3 (Apêndice 6) um resumo do TOT ERR.

Quadro 2: Códigos admissíveis nas transacções

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SER	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	—	—	—	—

▼B

Chave:

M = obrigatório

M* = apenas um dos dois tipos de registo pode ser incluído

O = facultativo

C = em função dos dados disponíveis

— = não permitido

1* = em função dos sistemas herdados

3.1.5. Campo 1.005: data de transacção (DOT)

Este campo indica a data em que a transacção foi iniciada e deve obedecer ao formato-padrão da ISSO: AAAAMMDD

sendo AAAA o ano, MM o mês e DD o dia do mês. Números com apenas um algarismo são precedidos de «0». Por exemplo «19931004» corresponde a 4 de Outubro de 1993.

3.1.6. Campo 1.006: prioridade (PRY)

Este campo facultativo define a prioridade do pedido numa escala de 1 a 9. «1» corresponde à prioridade máxima e «9» à mais baixa. As transacções com prioridade «1» devem ser tratadas imediatamente.

3.1.7. Campo 1.007: identificador do serviço de destino (DAI)

Este campo indica o serviço de destino da transacção.

É composto por dois elementos de informação no seguinte formato: CC/organismo.

O primeiro elemento contém o código de país, definido na norma 3166 da ISO, de dois caracteres alfanuméricos. O segundo, *organismo*, destina-se à identificação do organismo em texto livre com um número máximo de 32 caracteres alfanuméricos.

3.1.8. Campo 1.008: identificador do organismo de origem (ORI)

Este campo identifica o originador do ficheiro e tem o mesmo formato que o DAI (campo 1.007).

3.1.9. Campo 1.009: número de controlo da transacção (TCN)

Trata-se de um número de controlo para efeitos de referência. Deve ser gerado pelo computador e ter o seguinte formato: YYSSSSSSSA

sendo YY o ano da transacção, SSSSSSSS um número de série de oito algarismos e A uma letra de controlo gerada de acordo com o procedimento apresentado no Apêndice 2.

Na ausência de TCN, o campo YYSSSSSSSS é preenchido com zeros e a letra de controlo gerada de acordo com o procedimento acima descrito.

3.1.10. Campo 1.010: resposta de controlo da transacção (TCR)

Este campo facultativo contém o número de controlo da transacção da mensagem do pedido na resposta. Por conseguinte, apresenta o mesmo formato que o TCN (campo 1.009).

▼B

3.1.11. Campo 1.011: resolução de varrimento de origem (NSR)

Este campo indica a resolução de varrimento normal do sistema suportado pelo originador da transacção. Esta resolução é especificada com dois algarismos seguidos de um ponto decimal e mais dois algarismos.

Para todas as transacções efectuadas nos termos da Decisão 2008/615/JAI a taxa de amostragem deve ser de 500 píxeis/polegada ou 19,68 píxeis/mm.

3.1.12. Campo 1.012: resolução de transmissão nominal (NSR)

Este campo de cinco bytes especifica a resolução de transmissão normal para a transmissão das imagens. A resolução é expressa em píxeis/mm no mesmo formato que o NSR (campo 1.011).

3.1.13. Campo 1.013: nome de domínio (DOM)

Este campo obrigatório identifica o nome de domínio para a implementação do registo lógico de tipo-2 definido pelo utilizador. É composto por dois elementos de informação no seguinte formato: «INT-I{US}4.22{GS}».

3.1.14. Campo 1.014: Tempo Médio de Greenwich (GMT)

Este campo obrigatório prevê um mecanismo que permite indicar a data e a hora nas unidades universais do tempo médio de Greenwich (GMT). Quando utilizado, o campo GMT contém a data universal que constará para além da data local do campo 1.005 (DAT). A utilização do campo GMT elimina incoerências locais de tempo que surgem quando uma transacção e a respectiva resposta são transmitidas entre dois lugares separados por vários fusos horários. O GMT permite a indicação da data universal e das horas com relógio de 24 horas independentes dos fusos horários. É representado por «CCYYMMDDHHMMSSZ», uma sequência de 15 caracteres que corresponde à concatenação da data com o GMT e termina com a letra «Z». Os caracteres «CCYY» representam o ano da transacção, os caracteres «MM» as dezenas e unidades do mês e os caracteres «DD» as dezenas e unidades do dia do mês; os caracteres «HH» representam a hora, «MM» os minutos e «SS» os segundos. A data completa não deve exceder a data corrente.

4. ***Registo lógico de tipo-2: texto descritivo***

A estrutura da maior parte deste registo não é definida pela norma ANSI/NIST original. O registo contém informação de interesse específico para os serviços que transmitem ou recebem o ficheiro. A fim de assegurar a compatibilidade entre os serviços dactiloscópicos em comunicação, é necessário que o registo apenas contenha os campos adiante listados. Este documento especifica os campos que são obrigatórios e os que são facultativos e define também a estrutura de cada um dos campos.

4.1. *Campos do registo lógico de tipo-2*

4.1.1. Campo 2.001: comprimento de registo lógico (LEN — *Logical Record Length*)

Este campo obrigatório indica o comprimento do registo de tipo-2 e especifica o número total de bytes, incluindo todos os caracteres de todos os campos, bem como os separadores de informação.

4.1.2. Campo 2.002: carácter designador de imagem (IDC — *Image Designation Character*)

O IDC contido neste campo obrigatório é uma representação ASCII do IDC definido no campo conteúdo do ficheiro (CNT) do registo de tipo-1 (campo 1.003).

▼B

4.1.3. Campo 2.003: informação do sistema (SYS — *System Information*)

Este campo é obrigatório e contém 4 bytes que indicam a versão da INT-I aplicada por este registo específico de tipo-2.

Os primeiros dois bytes designam o número da versão principal, os dois seguintes, o número da revisão de importância secundária. Por exemplo, esta aplicação baseia-se na INT-I versão 4, revisão 22, e será portanto representada por «0422».

4.1.4. Campo 2.007: número de processo (CNO — *Case number*)

Trata-se de um número atribuído pelo serviço dactiloscópico local a um conjunto de latentes detectado no local de um crime. É adoptado o seguinte formado: *CC/número*,

em que *CC* é o código de país da Interpol, com dois caracteres alfanuméricos, e o *número* segue as directrizes locais adequadas, podendo comportar até um máximo de 32 caracteres alfanuméricos.

Este campo permite que o sistema identifique as imagens latentes associadas a um determinado crime.

4.1.5. Campo 2.008: número de sequência (SQN)

Este número designa cada sequência de imagens latentes num processo. Pode ter no máximo quatro algarismos. Uma sequência é composta de uma imagem latente ou uma série de imagens latentes, que são agrupadas para efeitos de arquivagem e/ou busca. Esta definição implica que mesmo as imagens latentes isoladas terão de receber um número de sequência.

Este campo pode ser incluído juntamente com o MID (Campo 2.009) para identificar uma determinada imagem latente numa sequência.

4.1.6. Campo 2.009: identificador de imagem latente (MID)

Este campo especifica uma determinada imagem latente numa sequência. O valor é uma única letra ou duas letras, sendo atribuída «A» à primeira latente, «B» à segunda e assim por diante até ao limite de «ZZ». Este campo é utilizado de forma análoga ao número de sequência de imagem latente referido acima para SQN (Campo 2.008).

4.1.7. Campo 2.010: número de referência criminal (CRN — *Criminal Reference Number*)

Trata-se de um número de referência único atribuído por um serviço nacional a uma pessoa acusada pela primeira vez de cometer uma infracção. Em cada país, ninguém tem mais de um CRN nem partilha esse número com nenhuma outra pessoa. Todavia, a mesma pessoa pode ter números de referência criminal em vários países que poderão ser distinguidos graças ao código de país.

É adoptado o seguinte formato para o campo CRN: *CC/número*,

em que *CC* é o código de país definido na ISSO 3166, com dois caracteres alfanuméricos, e o *número* segue as directrizes do serviços emitente, podendo comportar até um máximo de 32 caracteres alfanuméricos.

Para transacções no âmbito da Decisão 2008/615/JAI, este campo será utilizado para o número de referência criminal do serviço originador relacionado com as imagens nos registos de tipo-4 ou de tipo-15.

▼B

4.1.8. Campo 2.012: outro número de identificação (MN1)

Este campo contém o CRN (campo 2.010) transmitido numa transacção CPS ou PMS não antecedido do código do país.

4.1.9. Campo 2.013: outro número de identificação (MN2)

Este campo contém o CRN (campo 2.007) transmitido numa transacção MPS ou MMS não antecedido do código do país.

4.1.10. Campo 2.014: outro número de identificação (MN3)

Este campo contém o SQN (campo 2.008) transmitido numa transacção MPS ou MMS.

4.1.11. Campo 2.015: outro número de identificação misto (MN4)

Este campo contém o MID (campo 2.009) transmitido numa transacção MPS ou MMS.

4.1.12. Campo 2.063: informações complementares (INF)

Nas transacções de resposta SER a um pedido PMS, este campo incluirá informações sobre o dedo que está na origem do eventual acerto. O campo tem o seguinte formato:

NN, sendo *NN* o código de dois algarismos da posição dactilar definida no quadro 5.

Nos restantes casos, este campo é facultativo. É composto por até 32 caracteres alfanuméricos e pode dar informações suplementares sobre o pedido.

4.1.13. Campo 2.064: lista de respostas (RLS — *Respondents List*)

Este campo comporta pelo menos dois subcampos. O primeiro descreve o tipo de busca mediante as mnemónicas de três letras que indicam o tipo de transacção em TOT (campo 1.004). O segundo contém uma única letra. «I» para assinalar um acerto e «N» para indicar a ausência de concordância (não acerto). O terceiro subcampo inclui o identificador de sequência do resultado do candidato e o número total de candidatos separado por uma barra. Se existirem múltiplos candidatos, haverá múltiplas mensagens.

Na eventualidade de um acerto, o quarto subcampo conterá o resultado com até seis algarismos. Se o acerto tiver sido verificado é atribuído o valor de «999999» a este subcampo.

Exemplo: «CPS{RS}I{RS}001/001{RS}999999{GS}»

Se o AFIS remoto não atribuir nenhum resultado, deve ser utilizado um zero no ponto adequado.

4.1.14. Campo 2.074: Campo relativo ao estatuto/mensagem de erro (ERM)

Este campo contém mensagens de erro geradas nas transacções e que serão reenviadas ao requerente numa transacção de erro.

▼B

Quadro 3: Mensagens de erro

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.

Mensagens de erro com códigos de 100 a 199:

Estas mensagens de erro estão relacionadas com a validação dos registos ANSI/NIST e são definidas do seguinte modo:

<código de erro 1>: IDC <idc_número 1> CAMPO <identificador de campo 1> <texto dinâmico 1> LF

<código de erro 2>: IDC <idc_número 2> CAMPO <identificador de campo 2> <texto dinâmico 2>…

em que:

— o código de erro indica uma razão específica (ver quadro 3)

— o identificador de campo é o número de campo ANSI/NIST do campo errado (p.ex: 1.001, 2.001, ...) no formato <tipo de registo>.identificador de campo>.identificador de subcampo>

▼B

— o texto dinâmico é uma descrição dinâmica mais pormenorizada do erro

— LF é um espaço que separa erros caso sejam encontrados vários erros

— para o registo de tipo-1, o IDC é definido como «-1»

Exemplo:

201: IDC –1 CAMPO 1.009 CARACTER DE CONTROLO ERRADO {LF} 115: IDC 0 CAMPO 2.003 SISTEMA DE INFORMAÇÃO INVÁLIDO

Este campo é obrigatório nas transacções de erro.

4.1.15. Campo 2.320: número de candidatos pretendido (ENC)

Este campo contém o número máximo de candidatos para verificação pretendido pelo serviço requerente. O valor do ENC não pode exceder os valores definidos no quadro 11.

5. ***Registo lógico de tipo-4: imagens dactiloscópicas de alta resolução em escala de cinzentos***

Convém ter presente que os registos do tipo-4 têm sobretudo carácter binário e não ASCII. Por conseguinte, cada campo ocupa uma posição específica no registo, o que implica que todos os campos são obrigatórios.

A norma permite especificar no registo tanto a dimensão da imagem como a resolução. Os registos lógicos do tipo-4 devem conter dados de imagens dactiloscópicas que são transmitidas a uma resolução nominal de píxeis de 500 a 520 ppp. A taxa preferida para novas aplicações é uma densidade de 500 píxeis por polegada ou 19,68 píxeis por mm. 500 píxeis por polegada é a densidade especificada pela INT-I, embora sistemas semelhantes possam comunicar entre si a uma taxa diferente desde que se situe dentro do limite de 500 a 520 píxeis por polegada.

5.1. *Campos do registo lógico de tipo-4*

5.1.1. Campo 4.001: comprimento de registo lógico (LEN — *Logical Record Length*)

Este campo de quatro bytes indica o comprimento deste registo de tipo-4 e especifica o número total de bytes, incluindo todos os bytes de todos os campos contidos no registo.

5.1.2. Campo 4.002: carácter de designação da imagem (IDC — *Image Designation Character*)

Trata-se da representação binária do byte do número IDC indicado no ficheiro do cabeçalho.

5.1.3. Campo 4.003: tipo de impressão (IMP)

O tipo de impressão é um campo de um byte que ocupa o sexto byte do registo.

Quadro 4: Tipo de impressão digital

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

▼B

Code	Description
4	Latent impression captured directly
5	Latent tracing
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4. Campo 4.004: posição dactilar (FGP — Finger Position)

Este campo de comprimento fixo de 6 bytes ocupa as posições do sétimo ao décimo segundo byte de um registo do tipo-4. Contém as posições possíveis dos dedos com início no byte mais à esquerda (sétimo byte do registo). A posição dactilar conhecida ou mais provável é indicada de acordo com o quadro 5. Podem ser indicadas até cinco dedos suplementares, introduzindo as posições dos outros dedos nos cinco bytes restantes e utilizando o mesmo formato. Se forem utilizadas menos do que cinco referências de posições dactilares, os bytes não utilizados devem ser preenchidos com o binário 255. Para indicar todas as posições dactilares utiliza-se o código 0, que corresponde a «desconhecido».

Quadro 5: Código da posição dactilar e dimensão máxima

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

Para imagens latentes encontradas no local de um crime, devem ser utilizados apenas os códigos de 0 a 10.

▼B

5.1.5. Campo 4.005: resolução da imagem de varrimento (ISR — *Image Scanning Resolution*)

Este campo de um byte ocupa o décimo terceiro byte de um registo do tipo-4. O valor «0» indica que a imagem foi captada com a resolução preferida de 19,68 píxeis/mm (500 píxeis por polegada). O valor «1» indica que a imagem foi captada com uma resolução diferente especificada no registo de tipo-1.

5.1.6. Campo 4.006: comprimento horizontal da linha (HLL — *Horizontal Line Length*)

Este campo ocupa os bytes 14 e 15 no registo do tipo-4. Indica o número de píxeis contidos em cada linha digitalizada. O primeiro byte é o mais importante.

5.1.7. Campo 4.007: comprimento vertical da linha (HLL — *Vertical Line Length*)

Este campo regista nos bytes 16 e 17 o número de linhas digitalizadas presentes na imagem. O primeiro byte é o mais importante.

5.1.8. Campo 4.008: algoritmo de compressão em escala de cinzentos (GCA — *Gray-scale Compression Algorithm*)

Este campo de um byte indica o algoritmo de compressão em escala de cinzentos utilizado para codificar os dados da imagem. Para efeitos da presente aplicação, o código 1 indica que foi utilizada a compressão WSQ (apêndice 7).

5.1.9. Campo 4.009: a imagem

Este campo contém um fluxo de bytes que representa a imagem. A sua estrutura dependerá obviamente do algoritmo de compressão que for utilizado.

6. ***Registo lógico de tipo-9: registo de minúcias***

Os registos do tipo-9 conterão o texto ASCII que descreve as minúcias e informações conexas codificadas a partir de uma imagem latente. Para transacções de busca de latentes, o ficheiro pode conter um número indeterminado de registos de tipo-9, cada qual com uma visão ou imagem latente diferente.

6.1. *Extracção de minúcias*

6.1.1. Identificação do tipo de minúcia

Esta norma define os três números que identificam o tipo de minúcia. O quadro 6 enumera estes tipos. A terminação das cristas tem a designação de tipo 1. A bifurcação tem a designação de tipo 2. Se as minúcias não puderem ser classificadas claramente num dos dois tipos acima referidos, receberão a designação «outro», tipo 0.

Quadro 6: Tipos de minúcias

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Posição e tipo de minúcias

Para que os templates obedeçam aos requisitos da secção 5 da norma ANSI INCITS 378-2004, deve ser utilizado o seguinte método, que reforça a actual norma INCITS 378-2004, para determinar a posição (localização e orientação) de cada minúcia.

▼B

A posição ou localização de uma minúcia que representa uma terminação de crista será o ponto de bifurcação do esqueleto medial da zona do vale imediatamente à frente dessa terminação. Se as três pernas da zona do vale forem esqueletizadas para a largura de um píxel, o ponto de intersecção é a localização da minúcia. Do mesmo modo, a localização de uma minúcia constituída por uma bifurcação será o ponto de bifurcação do esqueleto medial da crista. Se as três pernas da crista forem esqueletizadas para a largura de um pixel, o respectivo ponto de intersecção é a localização da minúcia.

Quando todas as terminações de cristas tiverem sido convertidas em bifurcações, todas as minúcias da imagem dactiloscópica são representadas como bifurcações. As coordenadas X e Y do pixel da intersecção das três pernas de cada minúcia podem ser formatadas directamente. A determinação da orientação da minúcia pode ser deduzida de cada bifurcação esqueletizada. As três pernas de cada bifurcação esqueletizada devem ser analisadas e a terminação de cada perna deve ser determinada. A figura 6.1.2 ilustra os três métodos utilizados para determinar a terminação de uma perna com base numa resolução de varrimento de 500 ppp.

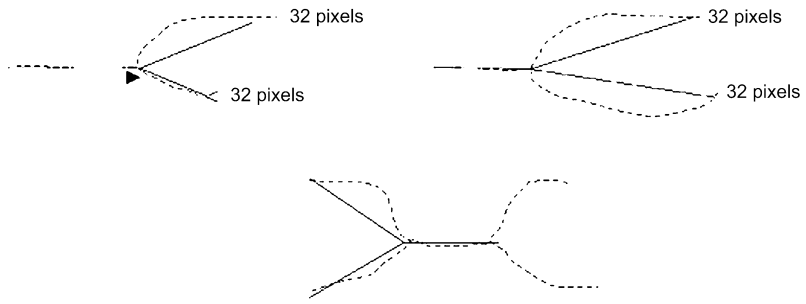
A terminação é determinada de acordo com o que vem primeiro. A contagem dos píxeis é feita com uma resolução de varrimento de 500 ppp. Resoluções de varrimento diferentes implicariam contagens diferentes.

— Uma distância de .064" (o 32.º pixel)

— A terminação da perna do esqueleto entre uma distância de .02" e .064" (do 10.º ao 32.º píxeis); não se utilizam pernas mais curtas

— Uma segunda bifurcação é encontrada numa distância de .064" (antes do 32.º píxel)

Figura 6.1.2



O ângulo das minúcias é determinado colocando três raios virtuais com início no ponto de bifurcação até à terminação de cada perna. O ângulo mais pequeno dos três ângulos formados pelos raio é cortado ao meio para indicar a orientação das minúcias.

6.1.3. Sistema de coordenadas

As minúcias de uma impressão digital devem ser determinadas num sistema de coordenadas cartesiano. A localização das minúcias será representada pelas respectivas coordenadas x e y. A origem do sistema de coordenadas será o canto superior esquerdo da imagem original com os eixos x e y que se estendem respectivamente para a esquerda e para baixo. As coordenadas x e y de uma minúcia serão representadas em unidades píxel a partir da origem. Convém notar que a localização da origem e das unidades de medidas não é compatível com a convenção utilizada nas definições do tipo-9 na norma ANSI/NIST-ITL 1-2000.

▼B

6.1.4. Orientação das minúcias

Os ângulos são expressos num formato matemático normalizado, com zero graus à direita e o aumento do ângulo orientado no sentido contrário ao dos ponteiros do relógio. Nas terminações de crista, os ângulos registados apontam no sentido para trás ao longo da crista e nas bifurcações no sentido do vale. Esta convenção está diametralmente oposta à convenção de ângulo descrita nas definições do tipo-9 na norma ANSI/NIST-ITL 1-2000.

6.2. *Campos do registo lógico de tipo-9 em formato INCITS-378*

Todos os campos do tipo-9 devem ser registados como texto ASCII. Neste registo de campo etiquetado não são permitidos campos binários.

6.2.1. Campo 9.001: comprimento de registo lógico (LEN — *Logical Record Length*)

Este campo ASCII obrigatório deve conter o comprimento do registo lógico que especifica o número total de bytes, incluindo cada um dos caracteres de todos os campos contidos no registo.

6.2.2. Campo 9.002: carácter de designação da imagem (IDC — *Image Designation Character*)

Este campo obrigatório de dois bytes destina-se à identificação e localização dos dados referentes às minúcias. O IDC contido neste campo obrigatório deve corresponder ao IDC encontrado no campo do conteúdo do registo de tipo-1.

6.2.3. Campo 9.003: tipo de impressão (IMP)

Este campo obrigatório de um byte destina-se a descrever a forma como a informação relativa à imagem dactiloscópica foi obtida. O valor ASCII do código adequado seleccionado do quadro 4 deve ser introduzido neste campo para indicar o tipo de impressão.

6.2.4. Campo 9.004: formato das minúcias (FMT)

Este campo conterá a letra «U», que indica que as minúcias estão formatadas de acordo com a norma M1-378. Embora a informação possa ser codificada de acordo com a norma M1-378, todos os campos de dados do registo do tipo-9 devem continuar a ser campos de texto ASCII.

6.2.5. Campo 9.126: informação CBEFF

Este campo deve conter três elementos de informação. O primeiro conterá o valor «27» (0x1B), ou seja, a identificação do proprietário do formato CBEFF atribuída pela Associação Internacional da Indústria Biométrica (IBIA) ao Comité Técnico M1 do INCITS. O caracter <US> separa este elemento do tipo de formato CBEFF que tem o valor de «513» (0x0201) para indicar que este registo apenas contém os dados relativos à localização e à orientação angular sem informações de bloco de dados estendido. O separador <US> separa este elemento do identificador de produto (PID) CBEFF que identifica o «proprietário» do equipamento de codificação. Este valor é estabelecido pelo vendedor e pode ser obtido do sítio internet da IBIA (www.ibia.org) a pedido.

6.2.6. Campo 9.127: identificação do equipamento de captação

Este campo conterá dois elementos de informação separados pelo carácter <US>. O primeiro com a menção «APPF» se o equipamento utilizado para captar a imagem foi certificado de acordo com o Apêndice F (IAFIS — *Image Quality Specification*, de 29 de Janeiro de 1999) do CJIS-RS-0010, *Federal Bureau of Investigation ' s Electronic Fingerprint Transmission Specification*. Se o equipamento não estiver conforme o campo ostentará a menção «NONE» (nada). O segundo elemento de informação conterá o identificador do equipamento de captação que é um número de produto atribuído ao vendedor do equipamento. O valor «0» indica a falta do identificador de equipamento.

▼B

6.2.7. Campo 9.128: comprimento horizontal da linha (HLL — *Horizontal Line Length*)

Este campo ASCI obrigatório conterá o número de píxeis numa linha horizontal da imagem transmitida. O comprimento horizontal máximo está limitado a 65 534 píxeis.

6.2.8. Campo 9.129: comprimento vertical da linha (HLL — *Vertical Line Length*)

Este campo ASCI obrigatório conterá o número de linhas horizontais da imagem transmitida. O comprimento vertical máximo está limitado a 65 534 píxeis.

6.2.9. Campo 9.130: unidades de escala (SLC — *Scale units*)

Este campo ASCII obrigatório indica as unidades utilizadas para descrever a frequência de captação da imagem (densidade de píxeis). O valor «1» neste campo indica o número de píxeis por polegada e o valor «2» o número de píxeis por centímetro. O valor «0» neste campo indica a ausência de escala. Nesse caso, o quociente de HPS/VPS indica o rácio do aspecto do pixel.

6.2.10. Campo 9.131: escala horizontal de píxeis (HPS — *Horizontal* pixel *scale*)

Este campo ASCII obrigatório deve conter a densidade total de píxeis na horizontal desde que o campo SLC ostente o valor «1» ou «2». Caso contrário, indica o componente horizontal do rácio do aspecto do pixel.

6.2.11. Campo 9.132: escala vertical de píxeis (VPS — *Vertical* pixel *scale*)

Este campo ASCII obrigatório deve conter a densidade total de píxeis na vertical desde que o campo SLC ostente o valor «1» ou «2». Caso contrário, indica o componente vertical do rácio do aspecto do pixel.

6.2.12. Campo 9.133: imagem dactilar

Este campo obrigatório indica o número da imagem do dedo correspondente aos dados deste registo. O número de imagem começa por «0» e vai de um a «15».

6.2.13. Campo 9.134: posição dactilar (FGP — *Finger position*)

Este campo deve indicar o código que identifica a posição dactilar que está na base da informação constante deste registo do tipo-9. Para indicar a posição dactilar ou palmar, deve ser utilizado um código de 1 a 10 do quadro 5 ou o código palmar adequado do quadro 10.

6.2.14. Campo 9.135: qualidade digital (*Finger quality*)

Este campo indica a qualidade geral dos dados relativos às minúcias digitais e os valores variam entre 0 e 100. Este número corresponde à avaliação geral da qualidade do registo digital e representa a qualidade da imagem original, da extracção das minúcias e eventuais operações suplementares que possam afectar o registo das minúcias.

6.2.15. Campo 9.136: número de minúcias

Este campo obrigatório contém a contagem do número de minúcias constantes deste registo lógico.

▼B

6.2.16. Campo 9.137: dados relativos às minúcias digitais (*Finger minutiæ data*)

Este campo obrigatório contém seis elementos de informação separados pelo carácter <US>. Compõe-se de vários subcampos, cada um dos quais contém os pormenores de minúcias individuais. O número total de subcampos deve corresponder à contagem indicada no campo 136. O primeiro elemento é constituído pelo número do índice das minúcias que começa em «1» e aumenta um valor para cada minúcia suplementar na impressão digital. Os segundos e terceiros elementos são as coordenadas «x» e «y» da minúcia expressas em unidades de píxeis. O quarto elemento de informação indica o ângulo das minúcias expresso em unidades de dois graus. Este valor deve ser um valor não negativo entre 0 e 179. O quinto elemento de informação identifica o tipo de minúcia. O valor «0» representa minúcias do tipo «OUTRAS», o valor «1» uma terminação de crista e o valor «2» uma bifurcação de crista. O sexto elemento indica a qualidade de cada minúcia. A variação máxima e mínima deste valor corresponde a 1 e 100, respectivamente. O valor «0» indica a ausência de valor de qualidade. Os subcampos devem ser separados com separadores <RS>.

6.2.17. Campo 9.138: informação relativa à contagem das cristas (*Ridge count information*)

Este campo é composto por uma série de subcampos, cada um dos quais contém três elementos de informação. O primeiro no primeiro campo indica o método de extracção da contagem de cristas. Um valor «0» indica que o método de extracção de contagem de cristas e a sua ordem no registo não devem ser tidos em conta. O valor «1» indica que, para cada ponto central de minúcia, os dados relativos à contagem de cristas foram extraídos até à minúcia mais próxima em quatro quadrantes e as contagens de cristas de cada centro de minúcia são agrupadas. O valor «2» indica que, para cada ponto central de minúcia, os dados relativos à contagem de cristas foram extraídos até à minúcia mais próxima em oito octantes e as contagens de cristas de cada centro de minúcia são agrupadas. Os restantes dois elementos do primeiro subcampo devem ambos ostentar o valor «0». Estes elementos devem ser separados pelo carácter <US>. Os subcampos seguintes contêm o número de índice do centro das minúcias como primeiro elemento, seguido do número de índice da minúcia adjacente e, por último, o número de cristas atravessadas. Os subcampos devem ser separados pelo carácter <US>.

6.2.18. Campo 9.139: informação sobre o ponto de referência (*Core information*)

Este campo contém um subcampo para cada ponto de referência presente na imagem original. Cada subcampo contém três elementos de informação. Os primeiros dois indicam as coordenadas «x» e «y» em unidades de píxeis. O terceiro elemento de informação indica o ângulo do ponto de referência expresso em unidades de dois graus. Este valor deve ser um valor não negativo entre 0 e 179. Vários pontos de referência devem ser separados pelo carácter <RS>.

6.2.19. Campo 9.140: Informação sobre os pontos delta (*Delta information*)

Este campo contém um subcampo para cada ponto delta presente na imagem original. Cada subcampo contém três elementos de informação. Os primeiros dois indicam as coordenadas «x» e «y» em unidades de píxeis. O terceiro elemento de informação indica o ângulo do ponto delta expresso em unidades de dois graus. Este valor deve ser um valor não negativo entre 0 e 179. Vários pontos de referência devem ser separados pelo carácter <RS>.

▼B

7. ***Registo de tipo 13 de imagens latentes de resolução variável***

O campo etiquetado do registo lógico de tipo-13 deve conter dados de imagens obtidos a partir de imagens latentes. Estas imagens serão enviadas aos serviços que extraem a informação pretendida das imagens quer automaticamente, quer por meio de intervenção e tratamento humanos.

As informações sobre a resolução de varrimento, a dimensão da imagem e outros parâmetros necessários ao tratamento da imagem constam de campos etiquetados no interior do registo.

Quadro 7: Tipo-13 — Formato do registo de imagens latentes de resolução variável

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
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	—	—	—	—	—	—

▼B

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
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	—

Chave do tipo de caracteres: N = numérico; A = alfabético; AN = alfanumérico; B = binário

7.1. *Campos do registo lógico de tipo-13*

Os parágrafos que se seguem descrevem os dados contidos em cada campo do registo lógico de tipo-13

No interior de um registo lógico de tipo-13, as entradas devem constar de campos numerados. Os primeiros dois campos do registo devem ser ordenados e o campo com os dados relativos à imagem deve constituir o último campo físico no registo. Para cada campo do registo de tipo-13, o quadro 7 indica o «código de condição» obrigatório «M» (*mandatory*) ou facultativo «O» (*optional*), o nome do campo, o tipo de caracteres, o tamanho do campo e os limites de ocorrência. O tamanho máximo em bytes do campo é dado na última coluna com um número de até três dígitos. O número de bytes aumenta em função do número de dígitos utilizados para o número de campo. As duas entradas na coluna «tamanho de campo por ocorrência» (*field size per occurrence*) incluem todos os separadores utilizados neste campo. A coluna «número máximo de bytes» (*maximum byte count*) inclui o número do campo, a informação e todos os separadores incluindo o carácter «GS».

7.1.1. Campo 13.001: comprimento de registo lógico (LEN — *Logical Record Length*)

Este campo ASCII obrigatório contém o número total de bytes de todo o registo lógico de tipo-13. O campo 13.001 indica o comprimento do registo, incluindo todos os caracteres de todos os campos contidos no registo, bem como os separadores de informação.

7.1.2. Campo 13.002: carácter de designação da imagem (IDC — *Image Designation Character*)

Este campo ASCI obrigatório destina-se a identificar os dados da imagem latente contidos no registo. Este IDC deve corresponder ao IDC encontrado no campo conteúdo (CNT) do registo de tipo-1.

7.1.3. Campo 13.003: tipo de impressão (IMP — *Impression type*)

Este campo ASCII obrigatório de um ou dois bytes destina-se a descrever a forma como a informação relativa à imagem latente foi obtida. Neste campo deve ser introduzido o código adequado de imagem latente do quadro 4 (impressões digitais) ou do quadro 9 (impressão palmar)

7.1.4. Campo 13.004: serviço originador/ORI (SRC) — *Source agency*

Este campo ASCII obrigatório conterá a identificação da administração ou entidade que captou em primeiro lugar a imagem facial contida no registo. Regra geral, constará deste campo o identificador do serviço originador (ORI) que captou a imagem. Compõe-se de dois elementos de informação com o seguinte formato: *CC/serviço*:

▼B

O primeiro elemento de informação contém o código de país da Interpol com dois caracteres alfanuméricos. O segundo elemento, *serviço*, é uma identificação do serviço em texto livre, que comporta até um máximo de 32 caracteres alfanuméricos.

7.1.5. Campo 13.005: data de captação da imagem latente (LCD — *Latent capture date*)

Este campo ASCI obrigatório deve indicar a data de captação da imagem latente contida no registo. A data deve ser indicada com oito algarismos no formato CCAAMMDD. A sequência «CCAA» corresponde ao ano em que a imagem foi captada; os caracteres «MM» representam as casas das décimas e unidades do mês e os caracteres «DD» as casas correspondentes às décimas e unidades do dia do mês. Por exemplo, «20000229» representa 29 de Fevereiro de 2000. A data completa deve ser uma data real.

7.1.6. Campo 13.006: comprimento horizontal da linha (HLL — *Horizontal Line Length*)

Este campo ASCI obrigatório indica o número de píxeis numa linha horizontal da imagem transmitida.

7.1.7. Campo 13.007: comprimento vertical da linha (HLL — *Vertical Line Length*)

Este campo ASCI obrigatório indica o número de linhas horizontais da imagem transmitida.

7.1.8. Campo 13.008: unidades de escala (SLC — *Scale units*)

Este campo ASCII obrigatório indica as unidades utilizadas para descrever a frequência de captação da imagem (densidade de píxeis). O valor «1» neste campo indica o número de píxeis por polegada e o valor «2», o número de píxeis por centímetro. O valor «0» neste campo indica a ausência de escala. Nesse caso, o quociente de HPS/VPS indica o rácio do aspecto do pixel.

7.1.9. Campo 13.009: escala horizontal de píxeis (HPS — *Horizontal* pixel *scale*)

Este campo ASCII obrigatório deve conter a densidade total de píxeis na horizontal desde que o campo SLC ostente o valor «1» ou «2». Caso contrário, indica o componente horizontal do rácio do aspecto do pixel.

7.1.10. Campo 13.010: escala vertical de píxeis (VPS — *Vertical* pixel *scale*)

Este campo ASCII obrigatório deve conter a densidade total de píxeis na vertical desde que o campo SLC ostente o valor «1» ou «2». Caso contrário, indica o componente vertical do rácio do aspecto do pixel

7.1.11. Campo 13.011: algoritmo de compressão (CGA — *Compression algorithm*)

Este campo ASCII obrigatório indica o algoritmo de compressão de imagens em tons de cinzento. Ver os códigos de compressão no Apêndice 7.

7.1.12. Campo 13.012: bits por pixel (BPX)

Este campo ASCII obrigatório indica o número de bits que representam um píxel. Este campo ostenta o número «8» para valores de tons de cinzento normais de «0» a «255». Um valor superior a «8» neste campo representa um píxel em escala de cinzentos com maior precisão.

▼B

7.1.13. Campo 13.013: posição dactilar/palmar (FGP — *Finger/palm position*)

Este campo etiquetado obrigatório deve conter uma ou mais posições dactilares ou palmares que possam corresponder à imagem latente. O número de código decimal correspondente às posições dactilares conhecidas ou mais prováveis ou à posição palmar mais conhecida deve ser tirado dos quadros 5 e 10, respectivamente, e introduzido como subcampo com um ou dois caracteres ASCII. As posições dactilares e/ou palmares suplementares podem ser indicadas introduzindo os códigos das outras posições como subcampos, separados pelo carácter de separação «RS». O código «0» para «dedo desconhecido» deve ser utilizado para indicar todas as posições dactilares de 1 a 10. O código «20» para «palma desconhecida» deve ser utilizado para indicar todas as posições de impressões palmares listadas.

7.1.14. Campo 13.014-019: reservado para definição futura (RSV — *Reserved for future definition*)

Estes campos estão reservados para serem incluídos em futuras revisões desta norma. Nenhum destes campos deve ser utilizado neste nível de revisão. Se qualquer destes campos estiver presente, deve ser ignorado.

7.1.15. Campo 13.020: comentários (COM)

Este campo facultativo pode servir para inserir comentários ou outras informações textuais ASCII com os dados de imagens latentes.

7.1.16. Campo 13.021-199: reservado para definição futura (RSV — *Reserved for future definition*)

Estes campos estão reservados para serem incluídos em futuras revisões desta norma. Nenhum destes campos deve ser utilizado neste nível de revisão. Se qualquer destes campos estiver presente, deve ser ignorado.

7.1.17. Campos 13.200-998: campos definidos pelo utilizador (UDF — *User-defined fields*)

Estes campos podem ser definidos pelos utilizadores e destinam-se a requisitos futuros. Os respectivos tamanho e conteúdo serão definidos pelo utilizador e devem ser compatíveis com o serviço receptor. Se estiverem presentes, devem conter informações textuais ASCII.

7.1.18. Campo 13.999: dados relativos às imagens (DAT — *Image data*)

Este campo incluirá todos dados relativos a uma imagem latente captada. Deve ostentar sempre o número de campo 999 e ser o último campo físico do registo. Por exemplo: ao número «13.999» seguem-se os dados da imagem em formato binário.

Cada píxel de dados não comprimidos em tons de cinzento deve ter até oito bits (256 tons de cinzento) num único byte. O número de bytes necessários para conter um píxel será diferente se o valor de BPX no campo 13.012 for superior ou inferior a «8». Em caso de compressão, os dados do píxel serão comprimidos de acordo com a técnica de compressão indicada no campo GCA.

7.2. *Terminação do registo de tipo-13 de imagens latentes de resolução variável*

Por uma questão de coerência, deve ser utilizado um separador «FS» entre o último byte de dados do campo 13.999 e o registo lógico seguinte. Este separador deve ser incluído no campo de comprimento do registo de tipo-13.

▼B

8. ***Registo de tipo-15 de imagens palmares de resolução variável***

O campo etiquetado de registo lógico de tipo-15 deve incluir e ser utilizado para efeitos de intercâmbio de dados de imagens palmares com campos de informação textual pré-estabelecidos e definidos pelo utilizador referentes à imagem digitalizada. As informações sobre a resolução de varrimento, a dimensão da imagem e outros parâmetros ou comentários necessários ao tratamento da imagem constam de campos etiquetados no interior do registo. As imagens palmares transmitidas a outros serviços serão tratadas pelos serviços receptores com vista a extrair a informação pretendida para efeitos de concordância.

Os dados das imagens devem ser colhidos directamente ao vivo (*live scan*) de uma pessoa com um sensor ou de um cartão com a impressão palmar ou outros suportes que contêm as impressões palmares da pessoa.

Qualquer que seja o método utilizado para obter imagens de impressões palmares, deve ser capaz de captar um conjunto de imagens de cada mão, nomeadamente a palma do escriba numa só imagem escaneada e toda a zona da palma desde o pulso até às extremidades dos dedos numa ou em duas imagens escanadas. Se forem utilizadas duas imagens para representar toda a palma, a imagem inferior deve reproduzir a área entre o pulso até ao topo da área interdigital (articulação metacarpo-falângica) e incluir as áreas tenar e hipotenar da palma. A imagem superior deve representar a área interdigital inferior até às extremidades dos dedos. Desde modo, assegura-se uma sobreposição adequada entre as duas imagens, ambas sobre a área interdigital da palma. Ao conferir a estrutura das cristas e minúcias contidas nesta área comum, o responsável pelo controlo pode concluir com elevado grau de certeza que se trata de imagens da mesma palma.

Dado que uma transacção de impressões palmares pode servir para fins diferentes, pode conter uma ou mais áreas para imagens da palma ou da mão. O conjunto completo de impressões palmares de uma pessoa incluirá de um modo geral a palma do escriba e a(s) imagem(ns) de toda a palma de cada mão. Uma vez que um campo etiquetado de registo lógico de imagem apenas pode conter um campo binário, será necessário um registo de tipo-15 para cada palma do escriba e um ou dois registos de tipo-15 para cada palma completa. Por conseguinte, serão necessários quatro a seis registos de tipo-15 para representar as impressões palmares de uma pessoa numa transacção normal.

8.1. *Campos do registo lógico de tipo-15*

Os parágrafos que se seguem descrevem os dados contidos em cada campo do registo lógico de tipo-15

No interior de um registo lógico de tipo-15, as entradas devem constar de campos numerados. Os primeiros dois campos do registo devem ser ordenados e o campo com os dados relativos à imagem deve constituir o último campo físico no registo. Para cada campo do registo de tipo-15, o quadro 8 indica o «código de condição» obrigatório «M» (*mandatory*) ou facultativo «O» (*optional*), o nome do campo, o tipo de caracteres, o tamanho do campo e os limites de ocorrência. O tamanho máximo em bytes do campo é dado na última coluna com um número de até três dígitos. O número de bytes aumenta em função do número de dígitos utilizados para o número de campo. As duas entradas na coluna «tamanho de campo por ocorrência» (*field size per occurrence*) incluem todos os separadores utilizados neste campo. A coluna «número máximo de bytes» (*maximum byte count*) inclui o número do campo, a informação e todos os separadores incluindo o carácter «GS».

▼B

8.1.1. Campo 15.001: comprimento de registo lógico (LEN — *Logical Record Length*)

Este campo ASCII obrigatório contém o número total de bytes de todo o registo lógico de tipo-15. O campo 15.001 indica o comprimento do registo, incluindo todos os caracteres de todos os campos contidos no registo, bem como os separadores de informação.

8.1.2. Campo 15.002: carácter de designação da imagem (IDC — *Image Designation Character*)

Este campo ASCI obrigatório destina-se a identificar a impressão palmar contida no registo. Este IDC deve corresponder ao IDC encontrado no campo conteúdo (CNT) do registo de tipo-1.

8.1.3. Campo 15.003: tipo de impressão (IMP — *Impression type*)

Este campo ASCII obrigatório de um byte destina-se a descrever a forma como a informação relativa à imagem palmar foi obtida. Deve ser introduzido neste campo o código adequado do quadro 9.

8.1.4. Campo 15.004: serviço originador/ORI (SRC) — *Source agency*

Este campo ASCII obrigatório conterá a identificação da administração ou entidade que captou em primeiro lugar a imagem facial contida no registo. Regra geral, constará deste campo o identificador do serviço originador (ORI) que captou a imagem. Compõe-se de dois elementos de informação com o seguinte formato: *CC/serviço*:

O primeiro elemento de informação contém o código de país da Interpol com dois caracteres alfanuméricos. O segundo elemento, *serviço*, é uma identificação do serviço em texto livre, que comporta até um máximo de 32 caracteres alfanuméricos.

8.1.5. Campo 15.005: data de captação da impressão palmar (PCD — *Palmprint capture date*)

Este campo ASCII obrigatório deve indicar a data de captação da imagem palmar. A data deve ser indicada com oito algarismos no formato CCAAMMDD. A sequência «CCAA» corresponde ao ano em que a imagem foi captada; os caracteres «MM» representam as casas das décimas e unidades do mês e os caracteres «DD» as casas correspondentes às décimas e unidades do dia do mês. Por exemplo, «20000229» representa 29 de Fevereiro de 2000. A data completa deve ser uma data real.

8.1.6. Campo 15.006: comprimento horizontal da linha (HLL — *Horizontal Line Length*)

Este campo ASCII obrigatório indica o número de píxeis numa linha horizontal da imagem transmitida.

8.1.7. Campo 15.007: comprimento vertical da linha (VLL — *Vertical Line Length*)

Este campo ASCII obrigatório indica o número de linhas horizontais da imagem transmitida.

8.1.8. Campo 15.008: unidades de escala (SLC — *Scale units*)

Este campo ASCII obrigatório indica as unidades utilizadas para descrever a frequência de captação da imagem (densidade de píxeis). O valor «1» neste campo indica o número de píxeis por polegada e o valor «2» o número de píxeis por centímetro. O valor «0» neste campo indica a ausência de escala. Nesse caso, o quociente de HPS/VPS indica o rácio do aspecto do píxel.

▼B

8.1.9. Campo 15.009: escala horizontal de píxeis (HPS — *Horizontal* pixel *scale*)

Este campo ASCII obrigatório deve conter a densidade total de píxeis na horizontal desde que o campo SLC ostente o valor «1» ou «2». Caso contrário, indica o componente horizontal do rácio do aspecto do píxel.

8.1.10. Campo 15.010: escala vertical de píxeis (VPS — *Vertical* pixel *scale*)

Este campo ASCII obrigatório deve conter a densidade total de píxeis na vertical desde que o campo SLC ostente o valor «1» ou «2». Caso contrário, indica o componente vertical do rácio do aspecto do pixel.

Quadro 8: Tipo-15 — Formato do registo de imagens palmares de resolução variável

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
COM	O	15.020	COMMENT	AN	2	128	0	1	128

▼B

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
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	—

Quadro 9: Tipo de impressão palmar

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. Campo 15.011: algoritmo de compressão (CGA — *Compression algorithm*)

Este campo ASCII obrigatório indica o algoritmo de compressão de imagens em tons de cinzento. A menção «NONE» (nada) neste campo indica que os dados deste registo não são comprimidos. Para as imagens que devem ser comprimidas, este campo indica o método preferido de compressão de imagens de conjuntos de impressões digitais (*tenprint*). Os códigos de compressão admitidos são definidos no Apêndice 7.

8.1.12. Campo 15.002: bits por píxel (BPX)

Este campo ASCI obrigatório indica o número de bits que representam um píxel. Este campo ostenta o número «8» para valores de tons de cinzento normais de «0» a «255». Um valor superior ou inferior a «8» neste campo representa um píxel em escala de cinzentos com maior ou menor precisão, respectivamente.

Quadro 10: Códigos, áreas e dimensões palmares

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

▼B

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Right Upper Palm	26	19 516	139,7	139,7
Left Lower Palm	27	19 516	139,7	139,7
Left Upper Palm	28	19 516	139,7	139,7
Right Other	29	28 387	139,7	203,2
Left Other	30	28 387	139,7	203,2

8.1.13. Campo 15.013: posição palmar (PLP — *Palm-print position*)

Este campo etiquetado obrigatório deve indicar a posição palmar que corresponde à imagem palmar. O número de código decimal correspondente às posições palmares conhecidas ou mais prováveis deve ser tirado do quadro 10 e introduzido como subcampo com um ou dois caracteres ASCII. O quadro 10 contém igualmente uma lista de áreas e dimensões máximas das imagens de cada posição palmar possível.

8.1.14. Campo 15.014-019: reservado para definição futura (RSV — *Reserved for future definition*)

Estes campos estão reservados para ser incluídos em futuras revisões desta norma. Nenhum destes campos deve ser utilizado neste nível de revisão. Se qualquer destes campos estiver presente, deve ser ignorado.

8.1.15. Campo 15.020: comentários (COM)

Este campo facultativo pode servir para inserir comentários ou outras informações textuais ASCII com os dados de imagens palmares.

8.1.16. Campo 15.021-199: reservado para definição futura (RSV — *Reserved for future definition*)

Estes campos estão reservados para ser incluídos em futuras revisões desta norma. Nenhum destes campos deve ser utilizado neste nível de revisão. Se qualquer destes campos estiver presente, deve ser ignorado.

8.1.17. Campos 15.200-998: campos definidos pelo utilizador (UDF — *User-defined fields*)

Estes campos podem ser definidos pelos utilizadores e destinam-se a requisitos futuros. Os respectivos tamanho e conteúdo serão definidos pelo utilizador e devem ser compatíveis com o serviço receptor. Se estiverem presentes, devem conter informações textuais ASCII.

8.1.18. Campo 15.999: dados relativos às imagens (DAT — *Image data*)

Este campo incluirá todos os dados relativos a uma imagem palmar captada. Deve ostentar sempre o número de campo 999 e ser o último campo físico do registo. Por exemplo: ao número «15.999» seguem-se os dados da imagem em formato binário. Cada píxel de dados não comprimidos em tons de cinzento deve ter até oito bits (256 tons de cinzento) num único byte. O número de bytes necessários para conter um píxel será diferente se o valor de BPX no campo 15.012 for superior ou inferior a «8». Em caso de compressão, os dados do píxel serão comprimidos de acordo com a técnica de compressão indicada no campo CGA.

▼B

8.2. *Terminação do registo de tipo-15 de imagens palmares de resolução variável*

Por uma questão de coerência, deve ser utilizado um separador «FS» entre o último byte de dados do campo 15.999 e o registo lógico seguinte. Este separador deve ser incluído no campo de comprimento do registo de tipo-15.

8.3. *Registo de tipo-15 suplementar de imagens palmares de resolução variável*

O ficheiro pode conter registos de tipo-15 suplementares. Por cada imagem palmar suplementar, é necessário um registo lógico de tipo-15 completo juntamente com o separador «FS».

Quadro 11: Número máximo de candidatos aceite para verificação por transmissão

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

Tipos de busca:

TP/TP: dez dedos contra dez dedos contra latente de impressão digital não identificada

LT/TP: latente de impressão digital contra dez dedos

LP/PP: latente de impressão palmar contra impressão palmar

TP/UL: dez dedos contra latente de impressão digital não identificada

LT/UL: latente de impressão digital contra latente de impressão digital não identificada

PP/ULP: impressão palmar contra impressão palmar não identificada

LP/ULP: latente de impressão palmar contra latente de impressão palmar não identificada

9. ***Apêndices do capítulo 2 (intercâmbio de dados dactiloscópicos)***

9.1. *Apêndice 1. Códigos de separação ASCII*

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

([1]) Posição definida na norma ASCII.

▼B

9.2. *Apêndice 2. Cálculo do carácter de controlo alfanumérico*

Para os campos TCN e TCR (campos 1.09 e 1.10):

O número que corresponde ao carácter de controlo é gerado mediante a seguinte fórmula:

(YY * $10^{8 + S}$SSSSSSS) Módulo 23,

onde YY e SSSSSSSS representam, respectivamente, o valor numerico dos últimos dois algarismos do ano e o número de série.

O carácter de controlo é gerado a partir da tabela de consulta *infra*.

Para o campo CRO (campo 2.010)

O número que corresponde ao carácter de controlo é gerado mediante a seguinte fórmula:

(YY * $10^{6 +}$ NNNNNN) Módulo 23,

onde YY e SSSSSSSS representam, respectivamente, o valor numérico dos últimos dois algarismos do ano e o número de série.

O carácter de controlo é gerado a partir do quadro de referência que se segue.

Tabela de consulta para os caracteres de controlo

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. *Apêndice 3. Códigos de caracteres*

Código ANSI de 7 bits para o intercâmbio de informações

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	{	|	}	~			

▼B

9.4. *Apêndice 4. Sumário das transacções*

Registo de Tipo-1 (obrigatório)

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

Na coluna relativa ao estatuto:

O = facultativo; M = obrigatório; C = condicional se a transacção for uma resposta ao serviço de origem

Registo de Tipo-2 (obrigatório)

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

▼B

Identifier	Field Number	Field Name	CPS/PMS	MPS/ /MMS	SRE	ERR
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	—	—

Na coluna relativa ao estatuto:

O = facultativo; M = obrigatório; C = condicional (caso haja dados disponíveis)

* = se a transmissão for compatível com a legislação nacional (não abrangida pela Decisão 2008/615/JAI)

9.5. *Apêndice 5. Registo de tipo-1 — definições*

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}

▼B

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
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

Na coluna relativa ao estatuto: O = facultativo, M = obrigatório, C = condicional

Na coluna relativa ao tipo de caracteres: A = letra, N = algarismo, B = binário

1* Os caracteres permitidos para o nome do serviço são os seguintes: [«0..9», «A..Z», «a..z», «_», «.», «», «—»]

9.6. *Apêndice 6. Registo de tipo-2 — definições*

Quadro A.6.1: Transacções CPS e PMS

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*	2063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Quadro A.6.2: Transacções SRE

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}

▼B

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
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}

Quadro A.6.3: Transacções ERR

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}

▼B

Quadro A.6.4: Transacções MPS e MMS

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}

Na coluna relativa ao estatuto: O = facultativo, M = obrigatório, C = condicional

Na coluna relativa ao tipo de caracteres: A = letra, N = algarismo, B = binário

1* Os caracteres permitidos são os seguintes: [«0..9», «A..Z», «a..z», «_», «.», «», «—»]

9.7. *Apêndice 7. Códigos de compressão em escala de cinzentos*

Códigos de compressão:

Compression	Value	Remarks
Wavelet Scalar Quantisation 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. *Apêndice 8. Requisitos de correio electrónico*

A fim de melhorar o processamento interno, devem constar do assunto de uma transacção no contexto de PRUEM o código do país (CC) do Estado-Membro que envia a mensagem e o tipo de transacção (TOT campo 1.004).

Formato: CC/tipo de transacção (TOT — *Type of Transaction*)

Exemplo: «DE/CPS»

O corpo da mensagem pode ficar vazio.

▼B

CAPÍTULO 3: **Intercâmbio de dados relativos ao registo de veículos**

1. ***Conjunto de dados comum para a busca automática de dados relativos ao registo de veículos***

1.1. *Definições*

As definições dos elementos obrigatórios e facultativos constantes do n.º 4 do artigo 16.º são os seguintes:

Obrigatório (M):

A informação deve ser comunicada se estiver disponível num registo nacional de um Estado-Membro. Existe, portanto, uma obrigação de trocar as informações caso estejam disponíveis.

Facultativo (O):

A informação pode ser comunicada se estiver disponível num registo nacional de um Estado-Membro. Não existe, portanto, nenhuma obrigação de trocar as informações mesmo se estiverem disponíveis.

Cada elemento dos dados identificado especificamente como sendo relevante no contexto da Decisão 2008/615/JAI recebe uma menção (Y).

1.2. *Busca de veículo/proprietário/detentor*

1.2.1. Disparadores (*triggers*) da busca

Existem duas maneiras diferentes de pesquisar a informação, nomeadamente:

— Por número do quadro (VIN), data e hora de referência (facultativo);

— Por número de matrícula, número do quadro (VIN) (facultativo), data e hora de referência (facultativo);

Graças a estes critérios de busca, serão dadas informações relativas a um e, por vezes, vários veículos. Se a resposta incluir informações acerca de apenas um veículo, todos os elementos são dados numa resposta. Se forem encontrados vários veículos, o Estado-Membro requerido pode determinar os elementos a incluir na resposta; ou seja, todos os elementos ou apenas os elementos destinados a afinar a busca (nomeadamente por razões de privacidade ou ligadas ao desempenho).

Os elementos necessários para afinar a busca são enumerados no ponto 1.2.2.1. Consta do ponto 1.2.2.2 o conjunto completo de informações.

A busca por número de quadro, data e hora de referência pode ser efectuada num ou em todos os Estados-Membros participantes.

A busca por número de matrícula, data e hora de referência pode ser efectuada num ou em todos os Estados-Membros participantes.

Regra geral, a busca será efectuada com a data e hora reais, mas é possível pesquisar com data e hora de referência no passado. Nesse caso, e se o registo do Estado-Membro em causa não incluir informações históricas porque essas informações não são registadas, podem constar da resposta os elementos actuais devidamente identificados como tais.

▼B

1.2.2. Conjunto de dados

1.2.2.1. Elementos a fornecer necessários para afinar a busca

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 = obrigatório se disponível no registo nacional, O = facultativo.
(2) Todos os atributos atribuídos especificamente pelos Estados-Membros são assinaladas com a letra «Y».
(3) Abreviatura de documento harmonizada, ver Directiva 1999/37/CE do Conselho, de 29 de Abril de 1999.

1.2.2.2. Conjunto completo de dados

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

▼B

Item	M/O (1)	Remarks	Prüm Y/N
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle.	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: — is the vehicle owner — is not the vehicle owner — is not identified by the registration certificate as being the vehicle owner	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y
Address	M	(C.2.3)	Y
Gender	M	male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm, etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date ownership	O	Start date of the ownership of the car.	N
End date ownership	O	End data of the ownership of the car.	N
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1) e.g. Ford, Opel, Renault, etc.	Y

▼B

Item	M/O (1)	Remarks	Prüm Y/N
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
Nature of the vehicle/EU Category Code	M	J) mopeds, motorbikes, cars, etc.	Y
Date of first registration	M	B) Date of first registration of the vehicle somewhere in the world	Y
Start date (actual) registration	M	I) Date of the registration to which the specific certificate of the vehicle refers	Y
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H).	Y
Status	M	scrapped, stolen, exported, etc.	Y
Start date status	M		Y
End date status	O		N
kW	O	(P.2)	Y
Capacity	O	(P.1)	Y
Type of licence number	O	regular, transito etc.	Y
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document	Y
Vehicle document id 2 (3)	O	A second document ID as printed on the vehicle document.	Y
Data relating to insurances			
Insurance company name	O		Y
Begin date insurance	O		Y
End date insurance	O		Y
Address	O		Y
Insurance number	O		Y
ID Number	O	An identifier that uniquely identifies the company.	N
Type of ID Number	O	The type of ID Number (e.g. number of the Chamber of Commerce)	N

(1) M = obrigatório se disponível no registo nacional, O = facultativo.
(2) Abreviatura de documento harmonizada, ver Directiva 1999/37/CE do Conselho, de 29 de Abril de 1999.
(3) No Luxemburgo, são utilizados dois documentos identificadores distintos para o registo automóvel.

▼B

2. ***Segurança da Informação***

2.1. *Síntese*

A aplicação Eucaris assegura a comunicação segura para os outros Estados-Membros e comunica com os sistemas *back-end* herdados dos Estados-Membros que utilizam a XML. Os Estados-Membros trocam mensagens directamente enviando-as ao destinatário. A central de dados de cada Estado-Membro está ligada à rede TESTA da União Europeia.

As mensagens XML enviadas via a rede são cifradas. Para tanto, é utilizada a técnica SSL (camada de conexão securizada). As mensagens enviadas ao *back-end* são mensagens textuais XML, uma vez que a conexão entre a aplicação e o *back-end* se processa num ambiente seguro.

É fornecida uma aplicação-cliente que pode ser utilizada no interior do Estado-Membro para efectuar buscas no próprio registo ou nos registos de outros Estados-Membros. Os clientes serão identificados mediante a identificação do utilizador/senha ou um certificado de cliente. A conexão ao utilizador pode ser cifrada, mas cabe a cada Estado-Membro tomar as medidas necessárias.

2.2. *Elementos de segurança relacionados com o intercâmbio de mensagens*

O esquema de segurança baseia-se numa combinação do protocolo HTTPS e a assinatura XML. No âmbito deste esquema, utiliza-se a assinatura XML para assinar todas as mensagens enviadas ao servidor e é possível autenticar o remetente da mensagem conferindo a assinatura. É utilizado um protocolo SSL unilateral (apenas um certificado de servidor) para proteger a confidencialidade e a integridade da mensagem em trânsito que oferece protecção contra tentativas de apagamento/reprodução e aditamento. Em vez de implementar, como previsto, o SSL bilateral, decidiu-se implementar a assinatura XML. A assinatura XML está mais próxima do roteiro de serviços *web* do que o SSL bilateral e tem, por conseguinte, vantagens estratégicas.

A assinatura XML pode ser implementada de diversas maneiras, mas a abordagem escolhida é utilizar a assinatura XML enquanto parte da segurança de serviços *web* (WSS). A WSS especifica a utilização da assinatura XML. Uma vez que a WSS está assente na norma SOAP, afigura-se lógico adoptar essa norma na medida do possível.

2.3. *Elementos de segurança não relacionados com o intercâmbio de mensagens*

2.3.1. Autenticação de utilizadores

Os utilizadores da aplicação *web* Eucaris autenticam-se mediante um nome de utilizador e uma senha. Uma vez que se utiliza a norma de autenticação Windows, os Estados-Membros podem aumentar o nível de autenticação dos utilizadores, se for caso disso, mediante certificados de clientes.

2.3.2. Papel de utilizador

A aplicação Eucaris suporta diferentes papéis de utilizador. Cada grupo tem a sua autorização específica. Por exemplo, os utilizadores (exclusivos) da funcionalidade «Acordo de Eucaris» não podem utilizar a funcionalidade «Prüm». Os serviços de administrador estão separados dos papéis de utilizadores finais normais.

▼B

2.3.3. Registar e reconstituir o intercâmbio de mensagens

A aplicação Eucaris permite o registo (*logging*) de todos os tipos de mensagens. A função de administrador permite ao administrador nacional determinar quais as mensagens que são registadas: pedidos dos utilizadores finais, pedidos recebidos de outros Estados-Membros, informações prestadas a partir dos registos nacionais, etc.

A aplicação pode ser configurada por forma a recorrer a uma base de dados interna para este efeito de registo ou a uma base de dados externa (Oracle). O tipo de mensagens a registar depende obviamente das outras facilidades de registo nos sistemas herdados e nas aplicações-cliente ligadas.

O cabeçalho de cada mensagem contém informações sobre o Estado-Membro requerente, o serviço requerente nesse Estado-Membro e o utilizador em causa. O motivo do pedido é igualmente assinalado.

Graças ao registo combinado no Estado-Membro requerente e no Estado-Membro que responde, é possível reconstituir na totalidade o intercâmbio de mensagens (p. ex. a pedido de um cidadão em causa).

O registo é configurado através do cliente *web* Eucaris (menu administração e configuração de registo). A funcionalidade de registo é efectuada pelo sistema central. Quando a função de registo está activada, a totalidade da mensagem (cabeçalho e corpo) é armazenada num registo. O nível de registo pode ser definido por serviço e pelo tipo de mensagem que passa pelo sistema central.

Níveis de registo

São possíveis os seguintes níveis de registo:

Privado — a mensagem é registada: o registo NÃO é acessível ao serviço de extracção de registos, sendo reservado ao nível nacional apenas para efeitos de auditorias e resolução de problemas.

Nada — A mensagem não fica registada.

Tipos de mensagens

O intercâmbio de informações entre Estados-Membros é composto por várias mensagens esquematizadas na figura *infra*.

Os tipos de mensagens possíveis (ilustradas na figura com o sistema central Eucaris do Estado-Membro X) são as seguintes:

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

▼B

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

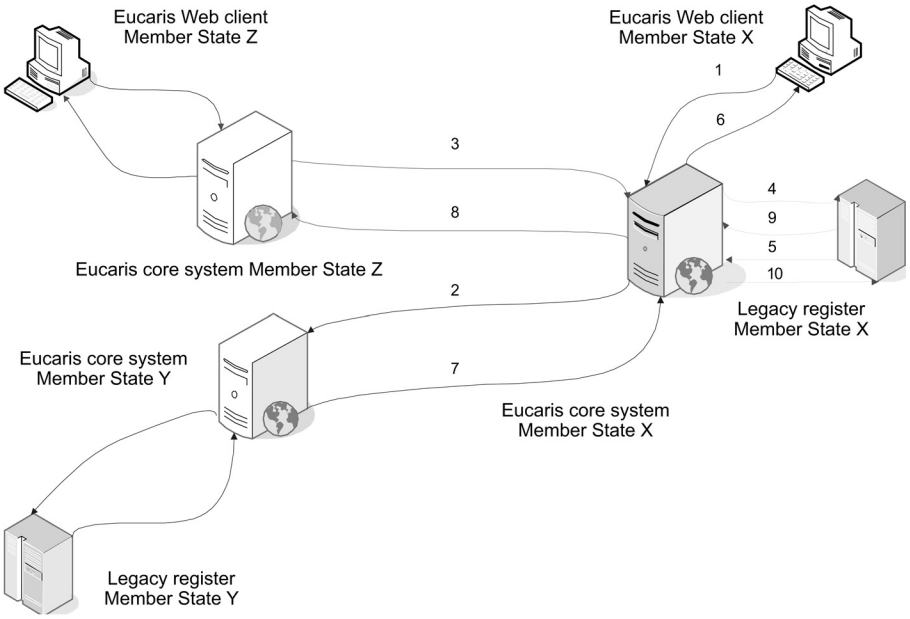
A figura ilustra os seguintes intercâmbios de informação:

— Pedido de informação do Estado-Membro X enviado ao Estado-Membro Y — setas azuis. Este pedido/resposta é composto por mensagens do tipo 1, 2, 7 e 6, respectivamente.

— Pedido de informação do Estado-Membro Z enviado ao Estado-Membro X — setas vermelhas. Este pedido/resposta é composto por mensagens do tipo 3, 4, 9 e 8, respectivamente.

— Pedido de informação do registo herdado para o respectivo sistema central (esta rota inclui um pedido de um cliente por detrás do registo herdado) — setas verdes. Este tipo de pedido é composto por mensagens do tipo 5 e 10.

Figura: tipos de mensagens para registo



2.3.4. Módulo de segurança do equipamento

Não é utilizado nenhum módulo de segurança do equipamento

Um módulo de segurança do equipamento (HMS — *Hardware Security Module*) fornece uma boa protecção para a chave utilizada para assinar mensagens e identificar servidores e aumenta o nível geral de segurança. Todavia, a sua aquisição/manutenção é onerosa e não há requisitos para optar para um FIPS 140-2 nível 2 ou HSM do nível 3. Uma vez que se utiliza uma rede fechada que atenua os riscos de forma eficaz, ficou decidido não utilizar um HMS no início. Se for necessário, por exemplo para efeitos de acreditação, pode ser acrescentado à arquitectura.

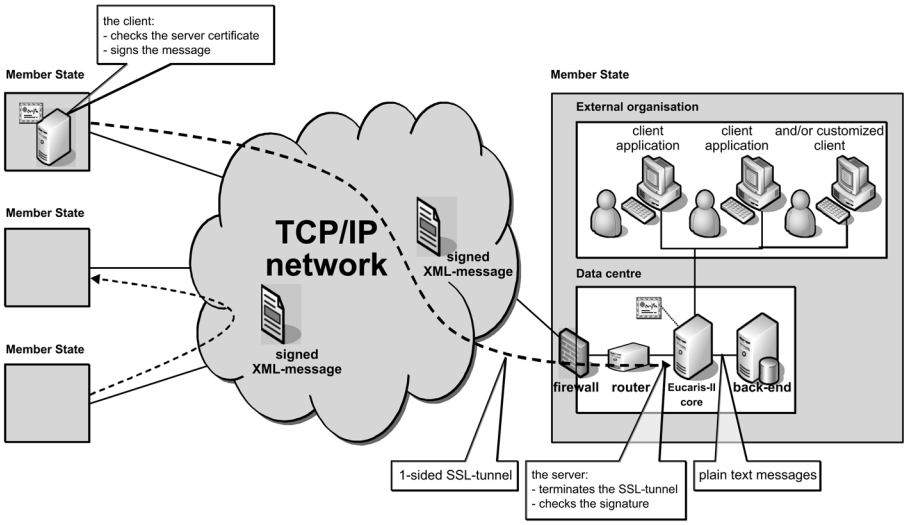
▼B

3. ***Condições técnicas para o intercâmbio de dados***

3.1. *Descrição geral da aplicação Eucaris*

3.1.1. Síntese

A aplicação Eucaris liga todos os Estados-Membros participantes numa rede malhada em que cada Estado-Membro comunica directamente com outro Estado-Membro. Não é necessária nenhum componente central para estabelecer a comunicação. A aplicação Eucaris assegura a comunicação segura para os outros Estados-Membros e comunica com os sistemas *back-end* herdados dos Estados-Membros que utilizam a XML. A seguinte imagem ilustra esta arquitectura.



Os Estados-Membros trocam mensagens directamente enviando-as ao destinatário. A central de dados de cada Estado-Membro está ligada à rede utilizada para o intercâmbio de mensagens (TESTA). Para aceder à rede TESTA, os Estados-Membros estabelecem a ligação através da sua porta nacional. Deve ser utilizada um corta-fogo para a ligação à rede e um encaminhador estabelece a ligação da aplicação Eucrais ao corta-fogo. Em função da opção escolhida para proteger as mensagens, é utilizado um certificado pelo encaminhador ou pela aplicação Eucaris.

É fornecida uma aplicação-cliente que pode ser utilizada no interior do Estado-Membro para efectuar buscas no próprio registo ou nos registos de outros Estados-Membros. A aplicação-cliente estabelece a ligação à Eucaris. Os clientes serão identificados mediante a identificação do utilizador/senha ou um certificado de cliente. A conexão a utilizadores numa organização externa (p.ex. polícia) pode ser cifrada, mas cabe a cada Estado-Membro tomar as medidas necessárias.

3.1.2. Âmbito do sistema

O sistema Eucaris está limitado aos processos envolvidos no intercâmbio de informações entre as autoridades de registo nos Estados-Membros e à apresentação básica dessas informações. Os procedimentos e processos automatizados da utilização da informação não são abrangidos pelo âmbito do sistema.

Os Estados-Membros podem optar por utilizar a funcionalidade cliente Eucaris ou criar a sua própria aplicação cliente adaptada. O quadro que se segue ilustra os aspectos obrigatórios do sistema Eucaris e/ou os aspectos facultativos e/ou que podem ser determinados pelos Estados-Membros.

▼B

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; — Authorisation of Member States and local users; — Routing of messages; — Queuing of asynchronous messages if the recipient service is temporally unavailable; — Multiple country inquiry functionality; — Logging of the exchange of messages; — Storage of incoming messages
Client application	O	In addition to the core application the Eucaris II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the Eucaris organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the Eucaris organisation and this Council Decision. The specifications can only be changed by the Eucaris organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the Eucaris organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

[1] M = uso ou cumprimento obrigatório O = uso ou cumprimento facultativo.

3.2. *Requisitos funcionais e não funcionais*

3.2.1. Funcionalidade genérica

Esta secção descreve as principais funções genéricas em termos gerais.

N.º	Descrição
1.	O sistema permite às autoridades de registo dos Estados-Membros trocar mensagens de pedidos e respostas de uma forma interactiva.
2.	O sistema integra uma aplicação-cliente que permite aos utilizadores finais enviar os seus pedidos e a informação da resposta para efeitos de tratamento manual.
3.	O sistema facilita a difusão, permitindo que um Estado-Membro possa enviar um pedido a todos os outros Estados-Membros. As respostas recebidas são consolidadas pela aplicação central numa mensagem de resposta à aplicação de cliente (esta funcionalidade é designada «*Multiple Country Inquiry*»)

▼B

N.º	Descrição
4.	O sistema pode lidar com diferentes tipos de mensagens. Os papéis dos utilizadores, a autorização, o encaminhamento, a assinatura e o acesso são todos definidos por cada serviço específico.
5.	O sistema permite aos Estados-Membros trocar lotes de mensagens ou mensagens que contenham um grande número de pedidos ou respostas. Estas mensagens são tratadas de modo assíncrono.
6.	O sistema coloca as mensagens assíncronas em lista de espera se o Estado-Membro destinatário estiver temporariamente indisponível e garante a entrega logo que o destinatário volte a ser disponível.
7.	O sistema armazena mensagens assíncronas até que possam ser tratadas.
8.	O sistema apenas dá acesso às aplicações Eucaris de outros Estados-Membros e não a serviços nesses Estados-Membros, ou seja, cada autoridade de registo desempenha o papel de passarela única entre os respectivos utilizadores finais nacionais e as autoridades congéneres nos outros Estados-Membros.
9.	É possível definir os utilizadores de diferentes Estados-Membros num servidor Eucaris e autorizá-los de acordo com os direitos desse Estado-Membro.
10.	As mensagens incluem informações relativas ao Estado-Membro requerente, o serviço e o utilizador final.
11.	O sistema permite registar o intercâmbio de mensagens entre os diferentes Estados-Membros e entre a aplicação central e os sistemas de registo nacionais.
12.	O sistema permite que um secretário, ou seja, uma organização ou um Estado-Membro explicitamente designado para o efeito, recolha informações registadas sobre mensagens enviadas/recebidas por todos os Estados-Membros participantes para elaborar relatórios estatísticos.
13.	Cada Estado-Membro assinala a informação registada que é disponibilizada ao secretário com classificação «privado».
14.	Este sistema permite aos administradores nacionais de cada Estado-Membro extrair estatísticas sobre a utilização.
15.	O sistema permite acrescentar novos Estados-Membros através de processos administrativos simples.

3.2.2. Facilidade de utilização

N.º	Descrição
16.	O sistema fornece uma interface de tratamento automatizado de mensagens graças a sistemas *back-end*/herdados e permite a integração interface do utilizador nesses sistemas (interface personalizada do utilizador).
17.	É fácil aprender a utilização do sistema que é convivial e fornece texto de apoio.
18.	O sistema inclui documentação para ajudar os Estados-Membros no que respeita a integração, actividades operacionais e manutenção futura (nomeadamente, manuais de referência, documentação funcional/técnica, manual operacional,…).
19.	A interface do utilizador é multilingue e permite ao utilizador final escolher a língua preferida.
20.	A interface do utilizador permite ao administrador local traduzir os elementos do ecrã e informações codificadas para a língua nacional.

▼B

3.2.3. Fiabilidade

N.º	Descrição
21.	O sistema é robusto e o seu funcionamento é fiável, tolera erros dos operadores e recupera sem problemas de cortes de energia ou outros incidentes. Deve ser possível relançar o sistema sem perda ou apenas com perdas mínimas de dados.
22.	O sistema deve produzir resultados estáveis e reproduzíveis.
23.	O sistema foi concebido para garantir a fiabilidade de funcionamento. É possível implementar o sistema numa configuração que garante uma disponibilidade de 98 % (por redundância, utilização de servidores de salvaguarda) em cada comunicação bilateral.
24.	É possível utilizar parte do sistema, mesmo com falha de alguns componentes (se o Estado-Membro não estiver operacional, os Estados-Membros A e B continuam a poder comunicar). O número de pontos de falhas na cadeia de informação deve ser reduzido ao mínimo.
25.	O tempo de recuperação após uma falha grave deve ser inferior a um dia. Deve ser possível minimizar a duração da inoperacionalidade mediante apoio remoto, nomeadamente um posto de serviço central.

3.2.4. Desempenho

N.º	Descrição
26.	O sistema pode ser utilizado 24 horas por dia, sete dias por semana. Esta disponibilidade (24x7) deve, por conseguinte, ser garantida também pelos sistemas herdados dos Estados-Membros.
27.	O sistema responde rapidamente a pedidos dos utilizadores independentemente de outras tarefas. É portanto necessário que os sistemas herdados das partes assegurem um tempo de resposta aceitável. Um tempo de resposta global de 10 segundos no máximo por pedido é aceitável.
28.	O sistema foi concebido como um sistema para múltiplos utilizadores e permite que possam continuar a ser desempenhadas tarefas de segundo plano enquanto o utilizador está ocupado com tarefas de primeira linha.
29.	O sistema foi concebido para suportar o aumento potencial do número de mensagens na eventualidade de serem acrescentadas novas funcionalidades ou novas organizações ou Estados-Membros.

3.2.5. Segurança

N.º	Descrição
30.	O sistema presta-se (graças às suas medidas de segurança) ao intercâmbio de mensagens que contenham dados pessoais sensíveis em termos de privacidade e que tenham a classificação «restrita» da União Europeia (p. ex. proprietários/detentores de veículos).
31.	A manutenção do sistema processa-se de molde a impedir o acesso não autorizado aos dados.
32.	O sistema inclui um serviço de gestão dos direitos e autorizações dos utilizadores finais nacionais.
33.	Os Estados-Membros podem verificar a identidade do remetente (a nível do Estado-Membro) graças à assinatura XML.

▼B

N.º	Descrição
34.	Os Estados-Membros devem dar uma autorização explícita a outros Estados-Membros para poderem pedir informações específicas.
35.	O sistema está dotado a nível da aplicação de um dispositivo pleno de segurança e de cifragem compatível com o nível de segurança exigido nestas circunstâncias. A exclusividade e a integridade da informação são garantidas graças à assinatura XML e à cifragem através do encaminhamento SSL.
36.	Todos os intercâmbios de mensagens podem ser reconstituídos através de registos.
37.	Existem seguranças contra tentativas de apagamento (apagamento por terceiros) e reprodução ou aditamento (reprodução ou aditamento por terceiros).
38.	O sistema recorre a certificados de Terceira Parte de Confiança (TTP — *Trusted Third Party*).
39.	O sistema pode suportar diferentes certificados dos Estados-Membros em função do tipo de mensagem ou serviço.
40.	As medidas de segurança a nível da aplicação são suficientes para permitir a utilização de redes não autorizadas.
41.	O sistema pode utilizar técnicas de segurança novas como um corta-fogo XML.

3.2.6. Adaptabilidade

N.º	Descrição
42.	Graças ao desenvolvimento central de componentes da aplicação, o sistema pode ser expandido e incluir novas mensagens e funcionalidades com custos de adaptação mínimos.
43.	Os Estados-Membros podem definir novos tipos de mensagens para fins bilaterais. Os Estados-Membros não são obrigados a suportar todos os tipos de mensagens.

3.2.7. Apoio e manutenção

N.º	Descrição
44.	O sistema inclui funções de monitorização atribuídas a um posto de serviço central e/ /ou operadores para a rede e os servidores nos diferentes Estados-Membros.
45.	O sistema permite o apoio remoto a partir de um posto de serviço central.
46.	O sistema inclui funcionalidades de análise de problemas.
47.	O sistema pode ser alargado a novos Estados-Membros.
48.	A aplicação pode ser instalada facilmente por pessoal dotado de um mínimo de qualificações e experiência IT. O processo de instalação é tanto quanto possível automatizado.
49.	O sistema inclui um ambiente permanente de testes e aceitação.
50.	Os custos anuais de manutenção e apoio foram reduzidos ao mínimo graças à utilização de normas de mercado e à concepção do sistema que exige um mínimo de apoio de um posto de serviço central.

▼B

3.2.8. Requisitos relativos ao projecto

N.º	Descrição
51.	O sistema foi concebido e está documentado para uma duração operacional de muitos anos.
52.	O sistema foi concebido por forma a torná-lo independente do prestador de serviços de rede.
53.	O sistema é compatível com os sistemas HW/SW nos Estados-Membros, utilizando uma tecnologia de rede aberta compatível com estes sistemas de registo (nomeadamente, XML, XSD, SOAP, WSDL, HTTP(s), serviços *web,* WSS, X.509).

3.2.9. Normas aplicáveis

N.º	Descrição
54.	O sistema é compatível com a protecção de dados conforme estabelecida no Regulamento (CE) 45/2001 (artigos 21.º, 22.º e 23.º) e na Directiva 95/46/CE.
55.	O sistema obedece às normas IDA.
56.	O sistema suporta caracteres UTF8.

CAPÍTULO 4: **Avaliação**

1. ***Procedimento de avaliação nos termos do artigo 20.º (preparação de decisões a que se refere o n.º 2 do artigo 25.º da Decisão 2008/615/JAI)***

1.1. *Questionário*

O grupo competente do Conselho deverá elaborar um questionário sobre cada intercâmbio automático de dados previsto no capítulo 2 da Decisão 2008/615/JAI.

Quando um Estados-Membros considerar que está preencher a totalidade de requisitos para o intercâmbio de dados na categoria de dados em causa, responderá ao questionário pertinente.

1.2. *Fase-piloto*

A fim de avaliar os resultados do questionário, os Estados-Membros que pretendam dar início à partilha de dados deverão lançar uma fase-piloto com um ou mais Estados-Membros que já estejam a partilhar dados ao abrigo da decisão do Conselho. A fase-piloto terá início imediatamente antes ou depois da visita de avaliação.

As condições e modalidades da fase-piloto serão estabelecidas pelo grupo competente do Conselho e basear-se-ão num acordo prévio com o Estados-Membros em causa. Os Estados-Membros que participem na fase-piloto determinarão as respectivas modalidades práticas.

1.3. *Visita de avaliação*

A fim de avaliar os resultados do questionário, será efectuada uma visita de avaliação aos Estados-Membros que pretendam dar início à partilha de dados.

As condições e modalidades desta visita serão estabelecidas pelo grupo competente do Conselho e basear-se-ão num acordo prévio entre o Estados-Membros em causa e a equipa de avaliação. O Estado-Membro em causa permitirá à equipa de avaliação verificar o intercâmbio automático de dados na ou nas categorias a avaliar, nomeadamente organizando um programa de visita que tenha em conta as pretensões formuladas pela equipa de avaliação.

▼B

No prazo de um mês, a equipa de avaliação apresentará um relatório sobre a visita de avaliação e submetê-lo-á ao Estado-Membro em causa para eventuais observações. Se for caso disso, este relatório será revisto pela equipa de avaliação à luz dos comentários do Estado-Membro.

A equipa de avaliação será composta por 3 peritos, no máximo, designados pelo Estado-Membro que participa no intercâmbio automático de dados nas categorias a avaliar, que tenham experiência no que respeita à categoria de dados em causa, tenham passado o controlo de segurança nacional para poder tratar destes assuntos e estejam dispostos a participar em pelo menos uma visita a outro Estado-Membro. A Comissão será convidada a integrar a equipa de avaliação na qualidade de observador.

Os membros da equipa de avaliação respeitarão a natureza confidencial da informação a que têm acesso no âmbito das suas funções.

1.4. *Relatório ao Conselho*

Será apresentado ao Conselho um relatório global com um resumo dos resultados dos questionários, da visita de avaliação e da fase-piloto a fim de que possa tomar a sua decisão nos termos do n.º 2 do artigo 25.º da Decisão 2008/615/JAI.

2. ***Procedimento de avaliação nos termos do artigo 21.º***

2.1. *Estatísticas e relatório*

Cada Estado-Membro compilará estatísticas sobre os resultados do intercâmbio automático de dados. A fim de assegurar a compatibilidade, o modelo de estatística será elaborado pelo grupo competente do Conselho.

Estas estatísticas serão transmitidas anualmente ao Secretariado-Geral, que elaborará uma síntese referente ao ano transacto, e à Comissão.

Além disso, os Estados-Membros deverão prestar periodicamente, no máximo uma vez por ano, informações suplementares sobre a implementação administrativa, técnica e financeira do intercâmbio automatizado de dados necessárias para analisar e melhorar o processo. Com base nestas informações será elaborado um relatório ao Conselho.

2.2. *Revisão*

Dentro de um prazo razoável, o Conselho analisará o mecanismo de avaliação aqui descrito e procederá à sua revisão se for caso disso.

3. Reuniões de peritos

No âmbito do grupo competente do Conselho, reunir-se-ão periodicamente peritos para organizar e implementar os procedimentos de avaliação acima referidos e para trocar experiências e debater possíveis melhorias. Se for caso disso, os resultados destes debates serão incorporados no relatório referido no ponto 2.1. *supra*.