DECISIÓN 2008/616/JAI DEL CONSEJO

de 23 de junio de 2008

relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el artículo 33 de la Decisión 2008/615/JAI del Consejo ([1]),

Vista la iniciativa de la República Federal de Alemania,

Visto el dictamen del Parlamento Europeo ([2]),

Considerando lo siguiente:

(1) El 23 de junio de 2008, el Consejo adoptó la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.

(2) Mediante la Decisión 2008/615/JAI, se incorporaron al ordenamiento jurídico de la UE los elementos básicos del Tratado de 27 de mayo de 2005 entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal (denominado en adelante «el Tratado de Prüm»).

(3) El artículo 33 de la Decisión 2008/615/JAI dispone que el Consejo adopte las medidas necesarias para la ejecución de dicha Decisión a escala de la Unión de conformidad con el procedimiento establecido en el artículo 34, apartado 2, letra c), segunda frase, del Tratado de la Unión Europea. Esas medidas deben basarse en el Acuerdo de ejecución administrativo y técnico del Tratado de Prüm de 5 de diciembre de 2006.

(4) La presente Decisión establece las disposiciones normativas comunes necesarias para la ejecución administrativa y técnica de las formas de cooperación establecidas en la Decisión 2008/615/JAI. El anexo de la presente Decisión contiene normas de desarrollo de carácter técnico. Por otra parte, la Secretaría General del Consejo elaborará y mantendrá actualizado un Manual independiente que contendrá exclusivamente información fáctica que deberán facilitar los Estados miembros.

(5) Teniendo en cuenta las capacidades técnicas, las consultas rutinarias de nuevos perfiles de ADN se realizarán en principio por medio de consultas simples y para ello se buscarán soluciones adecuadas a nivel técnico.

DECIDE:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objetivo

La presente Decisión tiene por objetivo establecer las disposiciones administrativas y técnicas necesarias para la ejecución de la Decisión 2008/615/JAI, en particular por lo que respecta al intercambio automatizado de datos de ADN, datos dactiloscópicos y datos de matriculación de vehículos, conforme a lo dispuesto en el capítulo 2 de dicha Decisión, y a otras formas de cooperación, conforme a lo dispuesto en su capítulo 5.

Artículo 2

Definiciones

A los efectos de la presente Decisión se entenderá por:

a) «consulta» y «comparación»: a tenor de los artículos 3, 4 y 9 de la Decisión 2008/615/JAI, los procedimientos mediante los cuales se determina si existe una concordancia entre los datos de ADN o los datos dactiloscópicos comunicados por un Estado miembro con datos de ADN o los datos dactiloscópicos almacenados en las bases de datos de otro, otros o todos los Estados miembros;

b) «consulta automatizada»: a tenor del artículo 12 de la Decisión 2008/615/JAI, un procedimiento de acceso en línea para consultar las bases de datos de otro, otros o todos los Estados miembros;

c) «perfil de ADN»: un código alfabético o numérico que representa un conjunto de características identificativas de la parte no codificante de una muestra de ADN humano analizada, es decir, la estructura molecular específica en los diversos loci (posiciones) de ADN;

d) «parte no codificante del ADN»: las regiones cromosómicas sin expresión genética, es decir, aquellas de cuya capacidad para determinar alguna propiedad funcional del organismo no se tiene constancia;

([1]) Véase la página 1 de este Diario Oficial.

([2]) Dictamen de 21 de abril de 2008 (no publicado aún en el Diario Oficial).

e) «índice de referencia de ADN»: un perfil de ADN y un número de referencia;

f) «perfil de ADN de referencia»: el perfil de ADN de una persona identificada;

g) «perfil de ADN no identificado»: el perfil de ADN obtenido a partir de vestigios obtenidos en el curso de la investigación de un delito y perteneciente a una persona aún no identificada;

h) «nota»: la marca que un Estado miembro añade a un perfil de ADN en su base de datos nacional que indica que ha habido una coincidencia con ese perfil de ADN a raíz de una consulta o comparación realizada por otro Estado miembro;

i) «datos dactiloscópicos»: las impresiones dactilares o las impresiones dactilares latentes, las impresiones palmares o las impresiones palmares latentes, y las plantillas de tales imágenes (codificación de las minucias), cuando están almacenadas y organizadas en una base de datos automatizada;

j) «datos de matriculación de vehículos»: el conjunto de datos especificados en el capítulo 3 del anexo de la presente Decisión;

k) «caso concreto»: a tenor del artículo 3, apartado 1, segunda frase, el artículo 9, apartado 1, segunda frase, y el artículo 12, apartado 1 de la Decisión 2008/615/JAI, un único expediente de investigación o de enjuiciamiento. Si el expediente contiene más de un perfil de ADN o más de un dato dactiloscópico o de matriculación de un vehículo, todos ellos podrán transmitirse juntos como una sola solicitud de consulta.

CAPÍTULO 2

DISPOSICIONES COMUNES PARA EL INTERCAMBIO DE DATOS

Artículo 3

Especificaciones técnicas

Los Estados miembros observarán las especificaciones técnicas comunes pertinentes para todas las solicitudes de consulta y respuestas relativas a consultas y comparaciones de perfiles de ADN, datos dactiloscópicos y datos de matriculación de vehículos. Dichas especificaciones técnicas se establecen en el anexo de la presente Decisión.

Artículo 4

Red de comunicaciones

El intercambio electrónico de datos de ADN, datos dactiloscópicos y datos de matriculación de vehículos entre los Estados miembros se efectuará empleando la red de comunicación de los Servicios transeuropeos de telemática entre administraciones (TESTA II) y las redes que se desarrollen ulteriormente a partir de ella.

Artículo 5

Disponibilidad del intercambio automatizado de datos

Los Estados miembros tomarán cuantas medidas sean necesarias para garantizar que puedan efectuarse consultas o comparaciones automatizadas de datos de ADN, datos dactiloscópicos y datos de matriculación de vehículos todos los días del año durante las 24 horas del día. De producirse un fallo técnico, los puntos de contacto nacionales de los Estados miembros se informarán de ello mutuamente y de inmediato, y convendrán en un sistema alternativo temporal de intercambio de información, de conformidad con la legislación vigente. El intercambio automatizado de datos se restablecerá lo antes posible.

Artículo 6

Números de referencia de los datos de ADN y los datos dactiloscópicos

Los números de referencia a que se refieren los artículos 2 y 8 de la Decisión 2008/615/JAI consistirán en una combinación de los siguientes elementos:

a) un código que, en caso de coincidencia, permita a los Estados miembros obtener, de sus propias bases de datos, datos personales y de otro tipo con el fin de facilitarlos a otro, otros o todos los Estados miembros, con arreglo a los artículos 5 o 10 de la Decisión 2008/615/JAI;

b) un código que indique la procedencia nacional del perfil de ADN o de los datos dactiloscópicos, y

c) por lo que respecta a los datos de ADN, un código que indique el tipo de perfil de ADN.

CAPÍTULO 3

DATOS DE ADN

Artículo 7

Principios aplicables al intercambio de datos de ADN

1. Los Estados miembros utilizarán las normas vigentes en materia de intercambio de datos de ADN, como el Conjunto de Normas Europeas (European Standard Set, ESS) o el Conjunto normalizado de loci de Interpol (Interpol Standard Set of Loci, ISSOL).

2. Para las consultas y comparaciones automatizadas de perfiles de ADN, el procedimiento de transmisión se efectuará dentro de una estructura descentralizada.

3. Se adoptarán las medidas oportunas para garantizar la confidencialidad e integridad de los datos que se envíen a otros Estados miembros, incluido su criptografiado.

4. Los Estados miembros tomarán las medidas necesarias para garantizar la integridad de los perfiles de ADN que se envíen o se pongan a disposición de los demás Estados miembros a efectos de comparación y velarán por que dichas medidas se atengan a normas internacionales como la norma ISO 17025.

5. Los Estados miembros emplearán los códigos de cada Estado miembro, de conformidad con la norma ISO 3166-1 alpha-2.

Artículo 8

Normas aplicables a las solicitudes de consulta y a las respuestas relacionadas con datos de ADN

1. Las solicitudes de consultas o comparaciones automatizadas contempladas en los artículos 3 y 4 de la Decisión 2008/615/JAI contendrán únicamente la siguiente información:

a) el código del Estado miembro que solicita la consulta;

b) la fecha, hora y el número de la solicitud;

c) los perfiles de ADN y sus números de referencia;

d) los tipos de perfiles de ADN transmitidos (perfiles no identificados o perfiles de referencia), y

e) la información necesaria para el control de los sistemas de bases de datos y el control de calidad de los procesos de búsqueda automatizada.

2. Las respuestas (informe sobre las coincidencias) a las solicitudes contempladas en el apartado 1 contendrán únicamente la siguiente información:

a) indicación de si se ha producido una, varias o ninguna coincidencia;

b) la fecha, hora y el número de la solicitud;

c) la fecha, hora y el número de la respuesta;

d) los códigos del Estado miembro que solicita la consulta y del que transmite la respuesta;

e) los números de referencia del Estado miembro que solicita la consulta y del que transmite la respuesta;

f) el tipo de perfiles de ADN transmitidos (perfiles no identificados o perfiles de referencia);

g) los perfiles de ADN solicitados y los perfiles de ADN que coinciden con ellos, y

h) la información necesaria para el control de los sistemas de bases de datos y el control de calidad de los procesos de búsqueda automatizada.

3. Solo se enviará notificación automatizada de una coincidencia si la consulta o comparación automatizada ha dado lugar a una coincidencia en un número mínimo de loci. Dicho mínimo se fija en el capítulo 1 del anexo de la presente Decisión.

4. Los Estados miembros velarán por que las solicitudes se ajusten a las declaraciones formuladas en virtud del artículo 2, apartado 3, de la Decisión 2008/615/JAI. Estas declaraciones figurarán en el Manual a que se refiere el artículo 18, apartado 2, de la presente Decisión.

Artículo 9

Procedimiento de transmisión en caso de consulta automatizada de perfiles de ADN no identificados de conformidad con el artículo 3 de la Decisión 2008/615/JAI

1. Si al realizar una consulta a partir de un perfil de ADN no identificado no se encuentran coincidencias en la base de datos nacional o se encuentra una coincidencia con un perfil de ADN no identificado, el perfil de ADN no identificado podrá transmitirse a las bases de datos de todos los demás Estados miembros, y si en una consulta a partir de este perfil de ADN no identificado se encuentran en las bases de datos de otros Estados miembros coincidencias con perfiles de ADN de referencia o no identificados, estas coincidencias se comunicarán automáticamente al Estado miembro que ha solicitado la consulta y se le transmitirán los índices de referencia de ADN; si en las bases de datos de los demás Estados miembros no se encuentran coincidencias, se comunicará automáticamente este hecho al Estado miembro solicitante.

2. Si al realizar una consulta a partir de un perfil de ADN no identificado se encuentra una coincidencia en las bases de datos de otros Estados miembros, cada uno de los Estados miembros de que se trate podrá añadir una nota en este sentido en su base de datos nacional.

Artículo 10

Procedimiento de transmisión en caso de consulta automatizada de perfiles de ADN de referencia de conformidad con el artículo 3 de la Decisión 2008/615/JAI

Si al realizar una consulta a partir de un perfil de ADN de referencia no se encuentra en la base de datos nacional ninguna coincidencia con un perfil de ADN de referencia o se encuentra una coincidencia con un perfil de ADN no identificado, este perfil de ADN de referencia podrá transmitirse a las bases de datos de todos los demás Estados miembros, y si en una consulta a partir de este perfil de ADN no identificado se encuentran en las bases de datos de otros Estados miembros coincidencias con perfiles de ADN de referencia o no identificados, estas coincidencias se comunicarán automáticamente al Estado miembro que ha solicitado la consulta y se le transmitirán los índices de referencia de ADN; si en las bases de datos de los demás Estados miembros no se encuentran coincidencias, se comunicará automáticamente este hecho al Estado miembro solicitante.

Artículo 11

Procedimiento de transmisión en caso de comparación automatizada de perfiles de ADN no identificados de conformidad con el artículo 4 de la Decisión 2008/615/JAI

1. Si al realizar una comparación con perfiles de ADN no identificados se encuentran en las bases de datos de otros Estados miembros coincidencias con perfiles de ADN de referencia o no identificados, estas coincidencias se comunicarán automáticamente al Estado miembro que ha solicitado la consulta y se le transmitirán los índices de referencia de ADN.

2. Si al realizar una comparación con perfiles de ADN no identificados se encuentran en las bases de datos de otros Estados miembros coincidencias con perfiles de ADN no identificados o de referencia, cada uno de los Estados miembros de que se trate podrá añadir una nota en este sentido en su base de datos nacional.

CAPÍTULO 4

DATOS DACTILOSCÓPICOS

Artículo 12

Principios aplicables al intercambio de datos dactiloscópicos

1. La digitalización de los datos dactiloscópicos y su transmisión a los demás Estados miembros se efectuará utilizando un formato de datos uniforme que se especifica en el capítulo 2 del anexo de la presente Decisión.

2. Cada Estado miembro se asegurará de que la calidad de los datos dactiloscópicos que transmite sea suficiente para realizar una comparación con los sistemas automáticos de identificación dactilar (SAID).

3. Para el intercambio de datos dactiloscópicos, el procedimiento de transmisión se efectuará dentro de una estructura descentralizada.

4. Se adoptarán las medidas oportunas para garantizar la confidencialidad e integridad de los datos dactiloscópicos que se envíen a otros Estados miembros, incluido su criptografiado.

5. Los Estados miembros emplearán los códigos de cada Estado miembro, de conformidad con la norma ISO 3166-1 alpha-2.

Artículo 13

Capacidades de búsqueda de datos dactiloscópicos

1. Cada Estado miembro velará por que sus solicitudes de consulta no excedan a las capacidades de búsqueda especificadas por el Estado miembro destinatario de la consulta. Los Estados miembros transmitirán a la Secretaría General del Consejo declaraciones conforme a lo dispuesto en el artículo 18, apartado 2, en las que harán constar sus capacidades de búsqueda máximas diarias de datos dactiloscópicos de personas identificadas y de datos dactiloscópicos de personas pendientes de identificación.

2. Los números máximos de candidatos sobre los que se aceptarán solicitudes de comprobación en cada transmisión se especifican en el capítulo 2 del anexo de la presente Decisión.

Artículo 14

Normas aplicables a las solicitudes de consulta y a las respuestas relacionadas con datos dactiloscópicos

1. El Estado miembro consultado comprobará sin demora la calidad de los datos dactiloscópicos transmitidos, utilizando un procedimiento plenamente automatizado. En caso de que los datos no se presten a una comparación automatizada, el Estado miembro consultado informará de ello sin tardanza al Estado miembro que ha formulado la consulta.

2. El Estado miembro consultado efectuará las búsquedas siguiendo el orden de recepción de las solicitudes. Las solicitudes deberán tramitarse en el plazo de 24 horas por un procedimiento plenamente automatizado. El Estado miembro que haya formulado la consulta podrá pedir, cuando así lo exija su Derecho interno, una tramitación urgente de sus solicitudes, en cuyo caso el Estado miembro consultado la realizará sin demora. Si no pueden cumplirse los plazos por causas de fuerza mayor, la comparación se efectuará sin demora una vez desaparecidos los impedimentos.

CAPÍTULO 5

DATOS DE MATRICULACIÓN DE VEHÍCULOS

Artículo 15

Principios aplicables a la consulta automatizada de datos de matriculación de vehículos

1. Para las consultas automatizadas de datos de matriculación de vehículos, los Estados miembros utilizarán una versión de la aplicación informática EUCARIS (sistema europeo de información sobre vehículos y permisos de conducción) concebida específicamente para los fines del artículo 12 de la Decisión 2008/615/JAI, y las versiones que se desarrollen ulteriormente a partir de dicha aplicación.

2. La consulta automatizada de datos de matriculación de vehículos se efectuará dentro de una estructura descentralizada.

3. La información que se intercambie a través del sistema Eucaris se transmitirá en forma cifrada.

4. Los elementos de datos de matriculación de vehículos que habrán de intercambiarse se especifican en el capítulo 3 del anexo de la presente Decisión.

5. Cuando apliquen el artículo 12 de la Decisión 2008/615/JAI, los Estados miembros podrán dar prioridad a las consultas relacionadas con la lucha contra la delincuencia grave.

Artículo 16

Gastos

Cada Estado miembro sufragará los gastos que se deriven de la administración, utilización y mantenimiento de la aplicación informática Eucaris mencionada en el artículo 15, apartado 1.

CAPÍTULO 6

COOPERACIÓN POLICIAL

Artículo 17

Patrullas conjuntas y otras operaciones conjuntas

1. De conformidad con el capítulo 5 de la Decisión 2008/615/JAI, y, en particular, con las declaraciones presentadas a tenor de su artículo 17, apartado 4, y su artículo 19, apartados 2 y 4, cada Estado miembro designará uno o más puntos de contacto para

que otros Estados miembros puedan dirigirse a las autoridades competentes y podrá especificar sus procedimientos para establecer patrullas conjuntas y otras operaciones conjuntas, sus procedimientos respecto de iniciativas de otros Estados miembros en relación con dichas operaciones, así como otros aspectos prácticos y operativos relacionados con tales operaciones.

2. La Secretaría General del Consejo recopilará y mantendrá actualizada la lista de puntos de contacto e informará a las autoridades competentes sobre cualquier cambio que se produzca en dicha lista.

3. Las autoridades competentes de cualquiera de los Estados miembros podrán tomar la iniciativa de llevar a cabo una operación conjunta. Antes de iniciarse una operación concreta, las autoridades competentes indicadas en el apartado 2, establecerán acuerdos escritos o verbales que podrán referirse a los siguientes aspectos:

a) las autoridades competentes de cada Estado miembro respecto de la operación;

b) el objetivo concreto de la operación;

c) el Estado miembro de acogida en el que se desarrollará la operación;

d) la zona geográfica del Estado miembro de acogida en la que se desarrollará la operación;

e) el período abarcado por la operación;

f) la colaboración concreta que deberán prestar al Estado miembro de acogida el Estado o los Estados miembros acreditantes, en forma de agentes u otros funcionarios, así como elementos materiales y financieros;

g) los agentes que participarán en la operación;

h) el agente responsable de la operación;

i) las competencias que los agentes y otros funcionarios de los demás Estados miembros acreditantes podrán ejercer en el Estado miembro de acogida durante la operación;

j) las armas, municiones y equipos concretos que podrán emplear los agentes acreditados a tenor de la Decisión 2008/615/JAI;

k) las condiciones logísticas en materia de transporte, alojamiento y seguridad;

l) el reparto de los costes de la operación conjunta, si se aparta de lo dispuesto en la primera frase del artículo 34 de la Decisión 2008/615/JAI;

m) cualquier otro elemento que pueda requerirse.

4. Las declaraciones, procedimientos y designaciones dispuestas en el presente artículo se consignarán en el Manual a que se refiere el artículo 18, apartado 2.

CAPÍTULO 7

DISPOSICIONES FINALES

Artículo 18

Anexo y Manual

1. El anexo de la presente Decisión establece más detalles sobre la ejecución técnica y administrativa de la Decisión 2008/615/JAI.

2. La Secretaría General del Consejo elaborará y mantendrá actualizado un Manual compuesto exclusivamente de información fáctica transmitida por los Estados miembros, bien mediante declaraciones a tenor de la Decisión 2008/615/JAI o de la presente Decisión, o bien mediante notificaciones a la Secretaría General del Consejo. El Manual asumirá la forma de un documento del Consejo.

Artículo 19

Órganos independientes de protección de datos

Los Estados miembros informarán a la Secretaría General del Consejo, de conformidad con el artículo 18, apartado 2, de la presente Decisión, acerca de los órganos independientes de protección de datos o las autoridades judiciales a que se refiere el artículo 30, apartado 5, de la Decisión 2008/615/JAI.

Artículo 20

Preparación de las decisiones contempladas en el artículo 25, apartado 2, de la Decisión 2008/615/JAI

1. El Consejo adoptará una decisión conforme a lo dispuesto en el artículo 25, apartado 2, de la Decisión 2008/615/JAI, basándose en un informe de evaluación que a su vez se basará en un cuestionario.

2. Por lo que respecta al intercambio automatizado de datos con arreglo al capítulo 2 de la Decisión 2008/615/JAI, el informe de evaluación se basará asimismo en una visita de evaluación y un ensayo piloto que se llevarán a cabo una vez que el Estado miembro al que corresponda haya informado a la Secretaría General conforme a lo dispuesto en la primera frase del artículo 36, apartado 2, de la Decisión 2008/615/JAI.

3. En el capítulo 4 del anexo de la presente Decisión se fijan otros detalles del procedimiento.

Artículo 21

Evaluación del intercambio de datos

1. Se efectuará periódicamente una evaluación de la ejecución administrativa, técnica y financiera del intercambio de datos a tenor del capítulo 2 de la Decisión 2008/615/JAI, y en particular de la utilización del mecanismo mencionado en el artículo 15, apartado 5. La evaluación versará sobre los Estados miembros que en el momento de realizarse esta apliquen ya la Decisión 2008/615/JAI, y se realizará respecto de las categorías de datos

para las cuales se haya iniciado ya el intercambio entre los Estados miembros interesados. La evaluación se basará en los informes de los Estados miembros respectivos.

2. En el capítulo 4 del anexo de la presente Decisión se fijan otros detalles del procedimiento.

Artículo 22

Relación con el Acuerdo de ejecución del Tratado de Prüm

Para los Estados miembros vinculados por el Tratado de Prüm, serán de aplicación las disposiciones pertinentes de la presente Decisión y de su anexo, tan pronto como se encuentren plenamente incorporadas en su Derecho interno, en lugar de las disposiciones correspondientes del Acuerdo de ejecución del Tratado de Prüm. Todas las demás disposiciones del Acuerdo de ejecución seguirán siendo de aplicación entre las Partes contratantes en el Tratado de Prüm.

Artículo 23

Ejecución

Los Estados miembros adoptarán las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión dentro de los plazos fijados en el artículo 36, apartado 1, de la Decisión 2008/615/JAI.

Artículo 24

Aplicación

La presente Decisión surtirá efecto a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Luxemburgo, el 23 de junio de 2008.

Por el Consejo

El Presidente

I. JARC

ANEXO

ÍNDICE

CAPÍTULO 1**: Intercambio de datos sobre el ADN**

1. ***Cuestiones criminalísticas relacionadas con el ADN, normas de comparación y algoritmos***

1.1. *Propiedades de los perfiles de ADN*

Los perfiles de ADN pueden contener 24 pares de números que representan a los alelos de 24 loci que también se utilizan en los procedimientos de ADN de Interpol. Los nombres de dichos loci figuran en el cuadro siguiente:

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

Los 7 loci sombreados en gris en la primera fila constituyen el actual conjunto europeo normalizado de loci (ESS) y el conjunto normalizado de loci de Interpol (ISSOL).

Normas de inclusión

Los perfiles de ADN facilitados por los Estados miembros para búsqueda y comparación, así como los perfiles de ADN enviados para búsqueda y comparación deben contener al menos 6 loci completamente determinados ([1]) y pueden contener loci adicionales o espacios en blanco, en función de su disponibilidad. Los perfiles de ADN de referencia deben contener al menos 6 de los 7 loci que constituyen el conjunto de normas europeas ESS. Para incrementar la exactitud de las comparaciones, todos los alelos disponibles se almacenarán en la base de datos de perfiles de ADN indexada y se utilizarán para la búsqueda y comparación. Los Estados miembros aplicarán tan pronto como sea posible en la práctica los nuevos loci del ESS que se adopten.

No están permitidos los perfiles mixtos, de forma que los valores de los alelos de cada loci consistirá en solo dos números que podrán ser los mismos en el caso de homocigosidad en loci concretos.

Los comodines («wild-cards») y las microvariantes deberán tratarse con arreglo a las normas siguientes:

— todo valor no numérico, excepto la amelogenina que contenga el perfil (por ejemplo, «o», «f», «r», «na», «nr» o «un») deberá convertirse automáticamente para la exportación a un comodín (*) y compararse con todos,

— los valores numéricos «0», «1» o «99» que contenga el perfil, deberán convertirse automáticamente para la exportación a un comodín (*) y compararse con todos,

— si se proporcionan 3 alelos para un loci, el primero de ellos se aceptará y los 2 alelos restantes deben convertirse automáticamente para su exportación a un comodín (*) y compararse con todos,

— cuando se proporcionan los valores de los comodines para los alelos 1 o 2, ambas permutaciones del valor numérico dado para el loci se compararán (por ejemplo, 12,* puede compararse con 12,14 o 9,12),

— las microvariantes de pentanucleótidos (Penta D, Penta E & CD4) se compararán de acuerdo con lo siguiente:

  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

— las microvariantes de tetranucleótidos (el resto de los loci son tetranucleótidos) se compararán de acuerdo con lo siguiente:

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

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

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

([1]) Por «completamente determinados» se entiende que se incluye el tratamiento de valores alelos raros.

1.2. *Normas de comparación*

La comparación de dos perfiles de ADN se hará sobre la base de los loci para los cuales se disponga de dos alelos en ambos perfiles de ADN. Por lo menos 6 loci completamente determinados (con exclusión de la amelogenina) deben coincidir en ambos perfiles de ADN antes de que se dé una respuesta positiva.

Una coincidencia total (calidad 1) se define como una coincidencia en la que son los mismos todos los valores de los alelos de los loci comparados que están contenidos normalmente en los perfiles de ADN solicitantes y solicitados. Una coincidencia aproximada se define como una coincidencia en la que solamente uno de los valores de los alelos comparados es distinto de los dos perfiles de ADN (calidad 2, 3 y 4). Una coincidencia aproximada solo se acepta si hay por lo menos 6 loci coincidentes completamente determinados en los dos perfiles de ADN comparados.

El motivo de una coincidencia aproximada puede ser:

— un error humano de mecanografía al introducir uno de los perfiles de ADN en la solicitud de búsqueda o en la base de datos de ADN,

— un error en la determinación de los alelos o un error de nomenclatura de alelos durante el proceso de generación del perfil de ADN.

1.3. *Normas de notificación*

Se notificarán tanto las coincidencias totales como las aproximadas y la ausencia total de coincidencia.

La notificación de coincidencia se remitirá al punto de contacto solicitante nacional y se pondrá también a disposición del punto de contacto nacional de transmisión (para que pueda hacer una estimación de la naturaleza y el número de posibles solicitudes de seguimiento para la obtención de más datos personales y otra información asociada al perfil de ADN que correspondan a la respuesta positiva, de conformidad con los artículos 5 y 10 de la Decisión 2008/615/JAI).

2. ***Cuadro de codificación de los Estados miembros***

De conformidad con la Decisión 2008/615/JAI, los códigos ISO 3166-1 alfa-2 se utilizan para establecer nombres de dominio y otros parámetros de configuración que se exigen en las aplicaciones de Prüm relativas al intercambio de datos de ADN en una red cerrada.

Los códigos ISO 3166-1 alfa-2 son los siguientes códigos de dos letras de los Estados miembros.

Nombres de los Estados miembros	Código	Nombres de los Estados miembros	Código
Bélgica	BE	Luxemburgo	LU
Bulgaria	BG	Hungría	HU
República Checa	CZ	Malta	MT
Dinamarca	DK	Países Bajos	NL
Alemania	DE	Austria	AT
Estonia	EE	Polonia	PL
Grecia	EL	Portugal	PT
España	ES	Rumanía	RO
Francia	FR	Eslovaquia	SK
Irlanda	IE	Eslovenia	SI
Italia	IT	Finlandia	FI
Chipre	CY	Suecia	SE
Letonia	LV	Reino Unido	UK
Lituania	LT		

3. ***Análisis funcional***

3.1. *Disponibilidad del sistema*

Las solicitudes con arreglo al artículo 3 de la Decisión 2008/615/JAI deberán acceder a la base de datos en el orden cronológico en el que se envió cada solicitud, y las contestaciones deberán enviarse de forma que lleguen al Estado miembro solicitante en el plazo de 15 minutos posterior a la recepción de la solicitud, supeditado a la calidad de funcionamiento de la red.

3.2. *Segunda etapa*

Cuando un Estado miembro recibe una notificación de coincidencia, corresponde a su punto de contacto nacional la comparación de los valores del perfil presentado como pregunta y los valores del perfil o de los perfiles recibidos como respuesta para validar y controlar el valor probatorio del perfil. Los puntos de contacto nacionales pueden ponerse en contacto entre sí directamente para la validación.

Los procedimientos de asistencia jurídica se inician tras la validación de una coincidencia existente entre dos perfiles, sobre la base de una «coincidencia total» o de una «coincidencia aproximada» obtenida durante la fase de consulta automatizada.

4. ***Documento de control del interfaz de ADN***

4.1. *Introducción*

4.1.1. Objetivos

Este capítulo determina los requisitos para el intercambio de información del perfil de ADN entre los sistemas de bases de datos de todos los Estados miembros. Los campos de encabezamiento se determinan de forma específica para el intercambio de ADN de Prüm. Los datos de identificación se basan en los datos de identificación del perfil de ADN en el esquema XML determinado para la pasarela de intercambio de ADN de Interpol.

Los datos se intercambian mediante SMTP (Protocolo simple de transferencia de correo) y otras tecnologías de última generación, utilizando un servidor central de retransmisión de correo, suministrado por el proveedor de red. El fichero XML se transporta como órgano de correo.

4.1.2. Ámbito de aplicación

Este documento de control del interfaz determina solo el contenido del mensaje (correo). Todas las cuestiones específicas de red y específicas de correo se determinan de forma uniforme para que haya una base técnica común para el intercambio de datos de ADN.

Esto incluye:

— el formato del campo del asunto del mensaje para permitir o posibilitar un tratamiento automatizado de los mensajes,

— el criptografiado del contenido cuando sea necesario y, en ese caso, los métodos que deban elegirse,

— la longitud máxima de los mensajes.

4.1.3. Estructuras y principios XML

El mensaje XML se estructura de la forma siguiente:

— zona de encabezamiento, que contiene información sobre la transmisión, y

— zona de datos de identificación, que contiene información específica del perfil, así como el propio perfil.

Se utilizará el mismo esquema de XML para la solicitud y la respuesta.

Para realizar los controles de los perfiles de ADN no identificados (artículo 4 de la Decisión 2008/615/JAI) se podrá enviar un lote de perfiles en un solo mensaje. Deberá determinarse un número máximo de perfiles para enviarse en un solo mensaje. Este número dependerá del tamaño máximo del correo permitido y se determinará tras haberse seleccionado el servidor de correo.

Ejemplo 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> datas structure repeated, if multiple profiles sent by

(….) a single SMTP message, only allowed for Art. 4 cases

</datas>]

</PRUEMDNA>

4.2. *Determinación de la estructura XML*

Las definiciones siguientes se proporcionan con efectos de documentación y para una mayor facilidad de lectura. La información vinculante real se proporciona en un archivo de esquema XML (PRUEM DNA.xsd).

4.2.1. Esquema PRUEMDNAx

Contiene los campos siguientes:

Campos	Tipo	Descripción
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 … 500

4.2.2. Contenido de la estructura del encabezamiento

4.2.2.1. Encabezamiento PRUEM

Es una estructura que describe el encabezamiento del archivo XML. Contiene los campos siguientes:

Campos	Tipo	Descripción
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. Info_encabezamiento_PRUEM

Tipo de datos contenidos en el mensaje, el valor puede ser:

Valor	Descripción
R	Solicitud

Valor	Descripción
A	Respuesta

4.2.2.3. Info_encabezamiento_PRUEM

Estructura para describir al Estado miembro así como fecha y hora del mensaje. Contiene los campos siguientes:

Campos	Tipo	Descripción
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. Contenido del dato del perfil PRUEM

4.2.3.1. Datos_PRUEM

Se trata de una estructura que describe los datos de identificación del perfil XML. Contiene los campos siguientes:

Campos	Tipo	Descripción
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. Tipo_solicitud_PRUEM

El tipo de datos contenidos en el mensaje. Pueden ser los siguientes:

Valor	Descripción
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_calidad_PRUEM

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

4.2.3.4. Tipo_ datos_PRUEM

Tipo de datos contenidos en el mensaje valores:

Valor	Descripción
P	Person profile
S	Stain

4.2.3.5. Resultado_datos_PRUEM

Tipo de datos contenidos en el mensaje, valores:

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

4.2.3.6. Perfil_ADN_IPSG

Estructura descriptiva de un perfil de ADN. Contiene los datos siguientes:

Campos	Tipo	Descripción
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_ADN_ISSOL

La estructura contiene los locus de ISSOL (Grupo normalizado de Locus de Interpol). Contiene los campos siguientes:

Campos	Tipo	Descripción
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Campos	Tipo	Descripción
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogenin

4.2.3.8. Locus_adicionales_ADN_IPSG

Estructura que contiene otros locus. Contiene los siguientes campos:

Campos	Tipo	Descripción
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. Locus_ADN_IPSG

Estructura que describe un locus. Contiene los campos siguientes:

Campos	Tipo	Descripción
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. ***Arquitectura de la solicitud, la seguridad y la comunicación***

5.1. *Generalidades*

Al tramitar las solicitudes para el intercambio de datos de ADN en el marco de la Decisión 2008/615/JAI, debe utilizarse una red de comunicación común que, lógicamente, será una red cerrada, limitada a los Estados miembros. Para explotar esta infraestructura de comunicación común para enviar solicitudes y recibir respuestas

de forma más eficaz, se adoptará un mecanismo asíncrono para transmitir solicitudes de datos de ADN y dactiloscópicos dactilares en un correo electrónico con arreglo al protocolo SMTP. Para cumplir los aspectos de seguridad, se utilizará el mecanismo MIME como extensión de la funcionalidad del SMTP para establecer un auténtico túnel seguro, de extremo a extremo, a lo largo de la red.

Se utiliza el sistema operativo TESTA (Servicios transeuropeos seguros de telemática entre administraciones, en inglés «Trans European Services for Telematic between Administrations») como red de comunicación para el intercambio de datos entre Estados miembros. TESTA está bajo la responsabilidad de la Comisión Europea. Teniendo en cuenta que las bases de datos nacionales de ADN y los actuales puntos de acceso de TESTA pueden estar situados en distintos lugares de los Estados miembros, el acceso a TESTA puede establecerse de una de las dos formas siguientes:

1) utilizando el punto de acceso nacional existente o estableciendo un nuevo punto de acceso nacional de TESTA, o bien

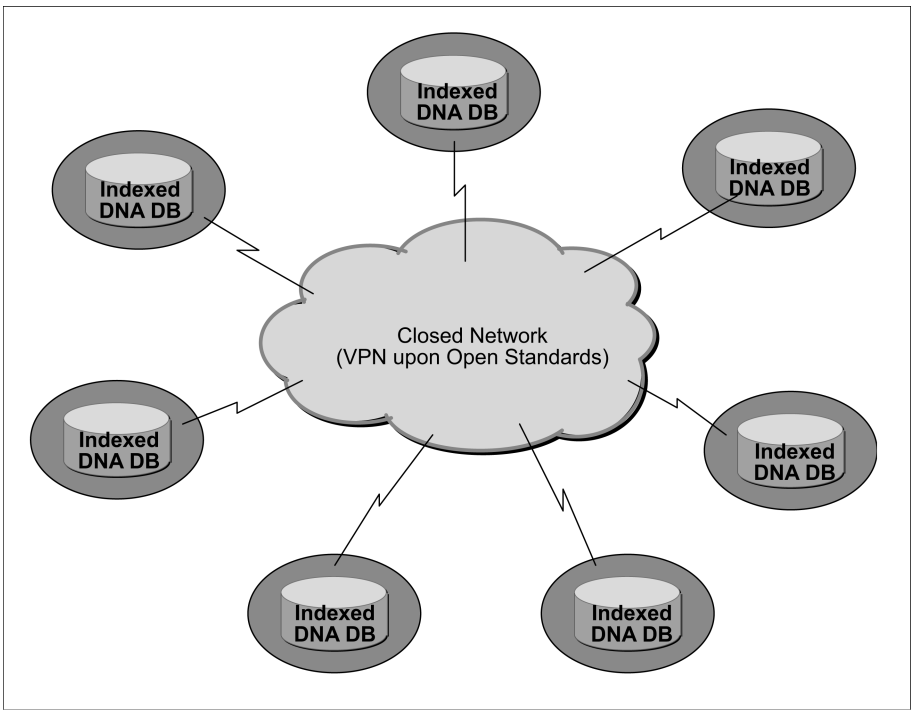
2) estableciendo un enlace local seguro con el punto de acceso nacional TESTA desde el lugar en el que se halle y se gestione por el organismo nacional competente la base de datos de ADN.

Los protocolos y normas utilizados para la ejecución de las aplicaciones de la Decisión 2008/615/JAI cumplen las normas abiertas y se ajustan a las exigencias que imponen los responsables políticos de la seguridad nacional de los Estados miembros.

5.2. *Arquitectura de nivel superior*

En el ámbito de aplicación de la Decisión 2008/615/JAI, cada uno de los Estados miembros pondrá a disposición sus datos de ADN para el intercambio con otros Estados miembros o cuando estos los requieran, con arreglo al formato de datos común normalizado. La arquitectura se basa en un modelo de comunicación entre los usuarios a escala individual. No existe ni un servidor informático central ni una base de datos centralizada para almacenar los perfiles de ADN.

Figura 1: Topología del intercambio de datos de ADN



Además del cumplimiento de las limitaciones legales nacionales en los sitios de los Estados miembros, cada uno de estos podrá decidir qué tipo de *hardware* y *software* se utilizará para la configuración de su sitio, de forma que se cumplan los requisitos que establece la Decisión 2008/615/JAI.

5.3. *Normas de seguridad y protección de datos*

Se han tenido en cuenta y aplicado tres niveles de seguridad.

5.3.1. Nivel de los datos

Los datos de perfiles ADN suministrados por los Estados miembros deberán prepararse de conformidad con una norma de protección de datos común, de forma que los Estados miembros solicitantes reciban una respuesta que indique, principalmente, RESPUESTA POSITIVA o NO HAY RESPUESTA POSITIVA, junto con un número de identificación en el primer caso, que no contenga ninguna información de carácter personal. La investigación subsiguiente a una notificación de RESPUESTA POSITIVA se hará a escala bilateral, de acuerdo con las reglamentaciones legales y organizativas nacionales existentes de los sitios de los respectivos Estados miembros.

5.3.2. Nivel de la comunicación

Los mensajes que contengan información sobre perfiles de ADN (solicitud y respuesta) se encriptarán mediante un sistema de última generación, con arreglo a normas abiertas, como el sistema MIME, antes de que se transmitan a los sitios de otros Estados miembros.

5.3.3. Nivel de la transmisión

Todos los mensajes cifrados que contengan información sobre perfiles de ADN se enviarán a los sitios de los demás Estados miembros a través de un sistema privado de túnel virtual administrado por un proveedor de red de categoría internacional de confianza y de los vínculos seguros con este sistema de túnel virtual bajo la responsabilidad nacional. Este sistema privado de túnel virtual no tendrá punto de conexión con la Internet abierta.

5.4. *Protocolos y normas que deben utilizarse para el mecanismo de cifrado: sMIME y paquetes conexos*

Se aplicará la norma abierta sMIME (Extensiones de correo de Internet de propósitos múltiples/seguro) como extensión de facto de la norma de correo electrónico SMTP para cifrar mensajes que contengan información sobre perfiles de ADN. El protocolo sMIME (V3) permite recibos firmados, etiquetas de seguridad, y listas de correo seguras y está estructurado sobre la base de la sintaxis de mensajes criptográficos (CMS), una especificación IETF para mensajes protegidos criptográficos. Puede utilizarse para firmar, resumir, autenticar o cifrar digitalmente cualquier forma de datos digitales.

El certificado subyacente utilizado por el mecanismo sMIME tiene que ajustarse a la norma X.509. A fin de asegurar normas y procedimientos comunes con otras aplicaciones de Prüm, las normas de tratamiento para operaciones de cifrado sMIME o para aplicación en los distintos entornos COTS (productos comerciales de serie), son las siguientes:

— la secuencia de las operaciones es: primero el cifrado y luego la firma,

— se aplicarán el algoritmo de cifrado AES (estándar de encriptación avanzada), de longitud clave de 256 bits, y RSA, de longitud clave de 1 024 bits, al cifrado simétrico y al asimétrico, respectivamente,

— se aplicará el algoritmo hash SHA-1.

La funcionalidad sMIME está incorporada en la gran mayoría de los paquetes de programas de correo electrónico modernos, incluidos Outlook, Mozilla Mail, así como Netscape Communicator 4.x y opera entre todos los principales paquetes de programas de correo electrónico.

Dada la facilidad de la integración de sMIME en la infraestructura nacional de TI de los sitios de todos los Estados miembros, se selecciona el mismo como mecanismo viable a fines de ejecución del nivel de seguridad de la comunicación. Sin embargo, para la realización del objetivo de «prueba de concepto» de una manera más eficaz y económica se elige el JavaMail API, de norma abierta, para el prototipo de intercambio de datos de ADN. El JavaMail API proporciona un cifrado y descifrado sencillos de los correos electrónicos que emplean sMIME u OpenPGP. Lo que se pretende es facilitar un único API de fácil uso a los clientes de correo electrónico que quieren enviar y recibir correo electrónico cifrado en cualquiera de los dos formatos más populares de cifrado de correo electrónico. Por lo tanto cualquier aplicación de última generación para JavaMail API será suficiente para satisfacer los requisitos establecidos por la decisión 2008/615/JHA, como el producto de Bouncy Castle JCE (siglas en inglés de extensión criptográfica de Java), que se utilizará para ejecutar sMIME a fines de creación de un prototipo de intercambio de datos de ADN entre todos los Estados miembros.

5.5. *Arquitectura de aplicación*

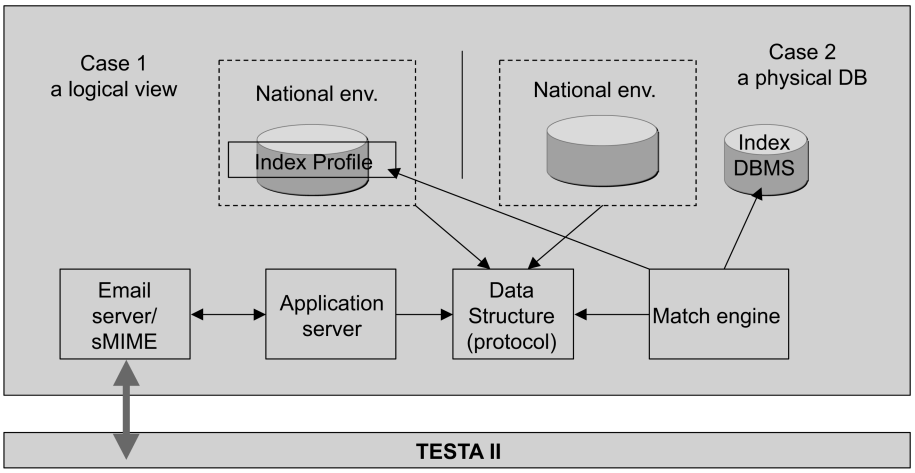
Cada Estado miembro facilitará a los demás Estados miembros de un conjunto de datos normalizados sobre el perfil de ADN conformes con el ICD (documento de control de la interfaz) común actual. Esto puede hacerse bien proporcionando una opinión lógica sobre la base de datos nacional individual, bien estableciendo una base de datos física exportada (base de datos en forma de registros).

Los cuatro componentes principales: el servidor de correo electrónico/sMIME, el servidor de la aplicación, el área de la estructura de los datos para la recogida y la alimentación de los datos y el registro de mensajes de entrada y de salida, y el motor de comparación ejecutan la lógica de la aplicación en su conjunto con independencia de los productos.

Con el objeto de facilitar a todos los Estados miembros una fácil integración de los componentes en sus respectivos sitios nacionales, la funcionalidad común especificada se ha ejecutado por medio de componentes libres, que podían ser seleccionados por cada Estado miembro en función de sus políticas y normativas nacionales en materia de Tecnología de la Información. A causa de las características independientes que deben ejecutarse para obtener el acceso a las bases de datos en forma de registros que contengan perfiles de ADN cubiertos por la Decisión 2008/615/JHA, cada Estado miembro puede libremente seleccionar su plataforma de soporte físico y programación, base de datos y sistemas operativos incluidos.

Un prototipo para el intercambio de datos de ADN ha sido desarrollado y probado con éxito sobre la red común existente. La versión 1.0 se ha desplegado en el entorno productivo y se utiliza para operaciones corrientes. Los Estados miembros pueden utilizar el producto desarrollado conjuntamente, pero pueden también desarrollar sus propios productos. Los componentes de productos comunes se mantendrán, se adaptarán a las necesidades particulares y se desarrollarán en función de la evolución de los requisitos de TI y de las exigencias de política científica o de funcionamiento policial.

Figura 2: Descripción de la topología de la aplicación



5.6. *Protocolos y normas que deben utilizarse para la arquitectura de aplicación*

5.6.1. XML

El intercambio de datos de ADN aprovechará completamente el esquema de XML como elemento adjunto a los mensajes de correo electrónico SMTP (Protocolo simple de transferencia de correo). El eXtensible Markup Language (XML) (lenguaje de anotación extensible) es un lenguaje de anotación de uso general recomendado por la pauta de accesibilidad del contenido en la Red W3C que sirve para crear lenguajes de anotación para usos especiales y es capaz de describir numerosos tipos de datos. La descripción del perfil de ADN conveniente para el intercambio entre todos los Estados miembros se ha efectuado mediante XML y del esquema XML en el documento DCI.

5.6.2. Conectividad abierta de bases de datos (siglas inglesas ODBC)

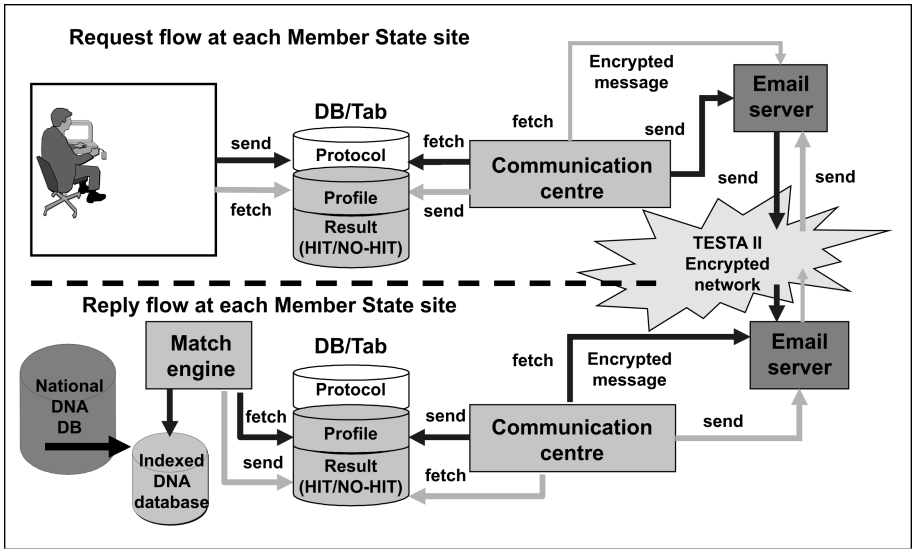
La conectividad abierta de bases de datos (Open DataBase Connectivity) es un método API de programación estándar para acceder a los sistemas de gestión de bases de datos que posee independencia respecto de los lenguajes de programación, las bases de datos y los sistemas operativos. La ODBC presenta, sin embargo, algunos inconvenientes. La administración de un gran número de máquinas clientes puede implicar una diversidad de programas instaladores y de bibliotecas de compartición de códigos (siglas inglesas DLL). Esta complejidad puede provocar un incremento del coste general de administración de sistema.

5.6.3. JDBC

La conectividad de base de datos Java (Java DataBase Connectivity) (JDBC) es un API (Interfaz de Programación de Aplicaciones) para el lenguaje de programación JAVA que define cómo puede acceder un cliente a una base de datos. A diferencia de ODBC, JDBC no necesita utilizar una serie de DLL locales en el escritorio.

En el siguiente diagrama se describe la lógica de las operaciones de formulación de solicitudes y envío de respuestas sobre perfiles de ADN en el sitio de cada Estado miembro. Tanto los flujos de solicitudes como los de respuestas interactúan con una zona de datos neutra que incluye distintos lotes comunes de datos con una estructura de datos común.

Figura 3: Sinopsis de los flujos de operaciones en el sitio de cada Estado miembro



5.7. *Entorno de comunicación*

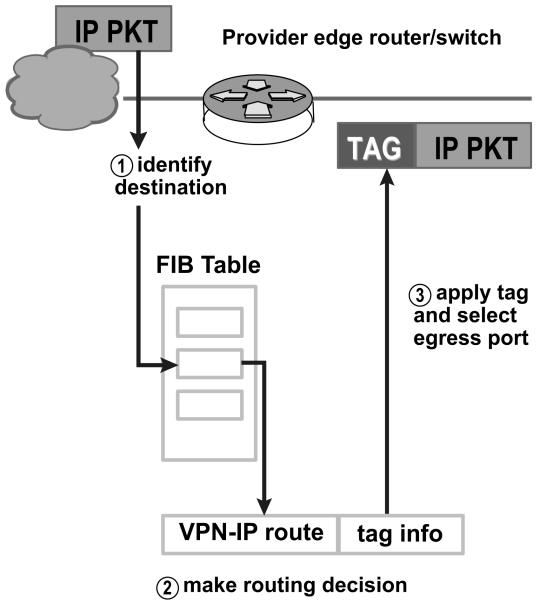
5.7.1. Red común de comunicación: TESTA y su infraestructura de aplicación

La aplicación de intercambio de datos de ADN utilizará el correo electrónico, un mecanismo asincrónico, para remitir solicitudes y recibir respuestas entre Estados miembros. Dado que todos los Estados miembros disponen como mínimo de un punto de acceso nacional a la red TESTA, el intercambio de datos sobre ADN se realizará a través de la red TESTA. TESTA proporciona una serie de servicios con valor añadido a través del correo electrónico. Además de albergar buzones específicos de correo electrónico de TESTA, la infraestructura puede realizar listas de distribución de correo y políticas de encaminamiento. Esto permite que TESTA se utilice como plataforma común para mensajes dirigidos a las administraciones conectadas a los dominios a escala de la UE. También pueden instalarse mecanismos de control de virus.

El relé de correo electrónico de TESTA está construido sobre una plataforma material de alta disponibilidad situada en las instalaciones centrales de la aplicación TESTA y protegida por un cortafuegos. El Servicio de Nombres de Dominio de TESTA (DNS) resolverá los localizadores de recursos en direcciones IP ocultando datos de envío del usuario y de las aplicaciones.

5.7.2. Aspectos de seguridad

El concepto de una VPN (Red Privada Virtual) se ha ejecutado en el marco de TESTA. La tecnología de conmutación por etiquetas (Tag Switching Technology) utilizada para construir este VPN evolucionará de modo que pueda aceptar la norma Conmutación de etiquetas multiprotocolo (Multi-Protocol Label Switching) (MPLS) desarrollada por el equipo especial de ingeniería de Internet (Internet Engineering Task Force) (IETF).



MPLS es una tecnología de norma IETF que acelera el flujo del tráfico de redes evitando el análisis de paquetes por encaminadores intermedios *(hops)*. Esto se consigue por medio de las denominadas etiquetas asociadas al paquete por los encaminadores de borde de la red troncal, basándose en la información almacenada en la base de información avanzada *(forwarding information base)* (FIB). Las etiquetas se utilizan también para ejecutar redes virtuales privadas (VPN).

MPLS combina las ventajas del encaminamiento de tres niveles con las de la conmutación de dos niveles. Dado que las direcciones IP no se evalúan durante el tránsito por la red troncal, MPLS no impone limitaciones de las direcciones IP.

Además, los mensajes de correo electrónico a través de TESTA estarán protegidos por el mecanismo de criptado basado en sMIME. Nadie que no conozca la clave ni disponga del certificado adecuado puede descifrar los mensajes en la red.

5.7.3. Protocolos y normas que deben utilizarse en la red de comunicación

5.7.3.1. SMTP

Simple Mail Transfer Protocol (protocolo simple de transferencia de correo) es la norma de facto para la transmisión de correo electrónico a través de Internet. SMTP es un protocolo relativamente simple, basado en textos, en el que se especifican uno o más receptores de un mensaje tras lo cual se transmite el mensaje. SMTP utiliza el puerto TCP 25 especificado por IETF. Para determinar el servidor SMTP para un nombre de dominio determinado, se utiliza el registro MX (Mail eXchange — intercambio de correo) DNS (Domain Name Systems — sistemas de nombres de dominio).

Dado que este protocolo empezó basándose estrictamente en texto ASCII no trataba adecuadamente los archivos binarios. Se desarrollaron normas como MIME para codificar archivos binarios con vistas a su transmisión a través de SMTP. Hoy en día, la mayoría de los servidores SMTP soportan las extensiones 8BITMIME y sMIME, que hacen posible que la transmisión de archivos binarios sea casi tan fácil como la de texto simple. Las reglas de tratamiento para operaciones sMIME se describen en la sección sMIME (véase el capítulo 5.4).

SMTP es un protocolo de transmisión automática («push») que no permite «descargar» mensajes de un servidor remoto a demanda del usuario. Para ello un cliente de correo debe utilizar POP3 o IMAP. En el marco de la realización de intercambio de datos de ADN se ha decidido utilizar el protocolo POP3.

5.7.3.2. POP

Los clientes locales de correo electrónico utilizan el protocolo Post Office Protocol versión 3 (POP3), un protocolo estándar de Internet a nivel de aplicación, para recuperar correo electrónico de un servidor remoto mediante una conexión TCP/IP. Al utilizar el perfil SMTP Submit del protocolo SMTP, los clientes de correo electrónico envían mensajes a través de Internet o de una red de empresa. MIME sirve de norma para los anexos y el texto de formato distinto de ASCII en el correo electrónico. Si bien ni POP3 ni SMTP requieren un correo electrónico con formato MIME, el correo electrónico de Internet está esencialmente formateado en MIME, de modo que los clientes POP también deben comprender y utilizar MIME. La totalidad del entorno de comunicación de la Decisión 2008/615/JAI incluirá por consiguiente los componentes de POP.

5.7.4. Adjudicación de direcciones de Red

Entorno operativo

La autoridad europea de registro de IP (RIPE) ha adjudicado a TESTA un bloque de subred de categoría C. En el futuro podrán asignarse a TESTA nuevos bloques si es necesario. La adjudicación de direcciones IP a los Estados miembros se basa en Europa en un esquema geográfico. El intercambio de datos entre Estados miembros en el marco de la Decisión 2008/615/JAI se lleva a cabo a través de una red IP europea con cierre lógico.

Entorno de prueba

A fin de establecer un entorno que funcione con agilidad para las operaciones diarias entre todos los Estados miembros conectados, es necesario establecer un entorno de prueba en la red cerrada para los nuevos Estados miembros que se preparan para unirse a las operaciones. Se ha determinado una hoja de parámetros que incluye direcciones IP, especificaciones de red, dominios de correo electrónico así como cuentas de usuarios de la aplicación, que debería configurarse en el sitio del Estado miembro correspondiente. Además, se ha elaborado a efectos de prueba una serie de perfiles de ADN ficticios.

5.7.5. Parámetros de configuración

Se ha configurado un sistema de correo electrónico seguro utilizando el dominio eu-admin.net. Este dominio, junto con las direcciones asociadas, no será accesible desde un lugar que no figure en el dominio TESTA de la UE, dado que los nombres solo se conocen en el servidor central DNS de TESTA, que está separado de Internet por una barrera.

La conversión de estas direcciones de sitio de TESTA *(host names)* en sus direcciones IP se lleva a cabo a través del servicio TESTA DNS. Para cada dominio local, se añadirá una entrada de correo a este servidor central DNS de TESTA, que retransmitirá a todos los mensajes de correo electrónico enviados a los dominios locales de TESTA al relé central de correo de TESTA. Este relé central de correo de TESTA los transmitirá seguidamente al servidor específico de correo electrónico del dominio local a través de las direcciones de correo electrónico del dominio local. Al retransmitir de este modo el correo electrónico, la información crítica contenida en el correo electrónico solo pasará a la infraestructura de red cerrada a escala europea y no al Internet inseguro.

Es necesario establecer dominios de rango inferior ***(negrita cursiva)*** en los sitios de todos los Estados miembros con arreglo a la siguiente sintaxis:

«***tipo de aplicación*.pruem.** ***Código de Estado miembro***.eu-admin.net», en la cual:

«Código de Estado miembro» corresponderá al valor de uno de los códigos de dos letras de los Estados miembros (por ejemplo: AT, BE etc.).

«Tipo de aplicación» corresponderá a uno de los siguientes valores: ADN y FP.

Si se aplica la sintaxis anterior, los dominios de rango inferior para los Estados miembros son los que figuran en la tabla siguiente:

EM	Dominios de rango inferior	Observaciones
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	***adn*.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	

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

EM	Dominios de rango inferior	Observaciones
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	……
	***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	

CAPÍTULO 2**: Intercambio de datos dactiloscópicos (documento de control de interfaz)**

El objetivo del siguiente Documento de Control de interfaces de documento es definir los requisitos para el intercambio de información dactiloscópica entre los sistemas informatizados de identificación de impresiones dactilares (AFIS) de dos Estados miembros. El documento se basa en la aplicación por parte de Interpol de ANSI/NIST-ITL 1-2000 (INT-I, Versión 4.22b).

Esta versión cubrirá todas las definiciones básicas de los registros lógicos de tipo-1, tipo-2, tipo-4, tipo-9, tipo-13 y tipo-15 necesarios para el tratamiento dactiloscópico basado en la imagen y los puntos característicos.

1. ***Sinopsis del contenido de los archivos***

Un archivo dactiloscópico está compuesto de varios registros lógicos. Existen 16 tipos de registros especificados en la norma original ANSI/NIST-ITL 1-2000. Los caracteres ASCII de separación adecuados se utilizan entre cada uno de los registros y los campos y subcampos dentro de cada uno de ellos.

Solo se utilizan seis tipos de registro para intercambiar información entre el servicio de origen y el destino:

Tipo-1 → información de transacción

Tipo-2 → datos alfanuméricos de personas y asuntos

Tipo-4 → imágenes dactiloscópicas en escalas de grises de alta resolución

Tipo-9 → registro de puntos característicos

Tipo-13 → registro de imágenes de resolución variable de huellas latentes

Tipo-15 → registro de resolución variable de impresiones palmares

1.1. *Tipo-1: Encabezamiento de archivo*

Este registro contiene información de encaminamiento e información descriptiva de la estructura del resto del archivo. Este tipo de registro define también los tipos de transacción que corresponden a una de las grandes categorías siguientes:

1.2. *Tipo-2: Texto descriptivo*

Este registro contiene información textual de interés para los servicios remitentes y receptores.

1.3. *Tipo-4: Imagen de alta resolución en escala de grises*

Este registro se utiliza para intercambiar imágenes dactiloscópicas de alta resolución en escalas de grises (8 bits) a 500 píxeles/pulgada. Las imágenes dactiloscópicas se comprimirán utilizando el algoritmo WSQ con una ratio que no superará 15:1. No deberán utilizarse otros algoritmos de compresión ni imágenes sin comprimir.

1.4. *Tipo-9: Registro de puntos característicos*

Los registros de tipo-9 se utilizan para intercambiar datos sobre peculiaridades de las crestas o puntos característicos. Su objetivo es, en parte, evitar una duplicación innecesaria de los procesos de codificación AFIS y, en parte también, permitir la transmisión de códigos AFIS con menos datos que las imágenes correspondientes.

1.5. *Tipo-13: Registro de imágenes de resolución variable de huellas latentes*

Este registro se utilizará para intercambiar imágenes de impresiones dactilares y palmares latentes junto con información alfanumérica sobre texturas. La resolución del barrido de las imágenes será de 500 píxeles/pulgada con 256 niveles de grises. Si la calidad de la imagen latente es suficiente, se comprimirá mediante el algoritmo WSQ. Si es necesario, la resolución de las imágenes puede expandirse a más de 500 píxeles/pulgada y más de 256 niveles de gris por acuerdo bilateral. En ese caso, se recomienda encarecidamente la utilización de JPEG 2000 (véase el apéndice 7).

1.6. *Registro de imágenes de resolución variable de impresiones palmares*

Los registros de campos etiquetados de tipo-15 se utilizarán para intercambiar imágenes de impresiones palmares de resolución variable. La resolución del barrido de las imágenes será de 500 píxeles/pulgada con 256 niveles de grises. Para reducir al mínimo la cantidad de datos todas las imágenes palmares se comprimirán mediante el algoritmo WSQ. Si es necesario, la resolución de las imágenes puede expandirse a más de 500 píxeles/pulgada y más de 256 niveles de gris por acuerdo bilateral. En ese caso, se recomienda encarecidamente la utilización de JPEG 2000 (véase el apéndice 7).

2. ***Formato del registro***

El archivo de intercambio estará compuesto de uno o varios registros lógicos. En cada registro lógico contenido en el archivo estarán presentes varios campos de información adecuados al tipo de registro. Cada uno de los campos de información podrá contener una o varias entradas de información básica de valor único. Estas entradas, una vez cotejadas, sirven para reflejar distintos aspectos de los datos que figuran en ese campo. Un campo de información puede también estar compuesto de una o varias entradas agrupadas y repetidas varias veces dentro de un mismo campo. Este grupo de entradas de información se conoce como un subcampo. Un campo de información puede consistir por consiguiente en uno o varios subcampos de entradas de información.

2.1. *Separadores de información*

En los registros lógicos de campos etiquetados, los mecanismos para delimitar la información se aplican mediante la utilización de separadores de información ASCII. La información delimitada podrá consistir en entradas de un campo o subcampo, campos de un registro lógico o múltiples ocurrencias de subcampos. Estos separadores de información se definen en la norma ANSI X3.4. Estos caracteres se utilizan para separar y calificar la información en un sentido lógico. Desde un punto de vista jerárquico, el carácter de separador de archivos «FS» es el más amplio, seguido del carácter de separador de grupos «GS», el carácter de separador de registros «RS», y por último el carácter de separador de unidades «US». En la tabla 1 figura una lista de separadores ASCII así como una descripción de su uso dentro de esta norma.

Los separadores de información deberían verse desde un punto de vista funcional como una indicación del tipo de datos siguiente. El carácter «US» separará entradas de información dentro de un campo o subcampo. Es una indicación de que la siguiente entrada de información será un ejemplar de dato correspondiente a este campo o subcampo. Múltiples subcampos dentro de un campo separados por el carácter «RS» indican el comienzo del siguiente grupo de entradas de información reiteradas. El carácter separador «GS» utilizado entre campos de información indica el comienzo de un nuevo campo que precede al número identificador del campo que aparezca. Del mismo modo, el comienzo de un nuevo registro lógico se indicará mediante la aparición del carácter «FS».

Los cuatro caracteres solo tienen un significado cuando se utilizan como separadores de entradas de datos en los campos de registros de texto ASCII. No existe una significación específica de estos caracteres cuando aparecen en registros binarios de imagen y en campos binarios, solo forman parte de los datos intercambiados.

Normalmente, no debería haber campos y entradas de información vacíos, por lo cual solo debería aparecer un separador entre dos entradas de datos. La excepción a esta regla se presenta en aquellos casos en que los datos que figuran en los campos o en las entradas de información no están disponibles, han desaparecido o son facultativos y el tratamiento de la transacción no depende de la presencia de estos datos en concreto. En tales casos, varios caracteres de separación adyacentes aparecerán juntos en lugar de que sea necesaria la inserción de datos sin sentido entre los caracteres separadores.

Para la definición de un campo consistente en tres entradas de información, se aplica el procedimiento siguiente. Si falta la información para la segunda entrada de información, figurarán dos caracteres separadores de información «US» adyacentes entre la primera y la tercera entrada de información. Si faltan tanto la segunda como la tercera entrada de información, se utilizarán tres caracteres separadores, dos caracteres «US» además del carácter separador que indica el final del campo o subcampo. En general, si no se dispone de una o varias entradas de información obligatorias u opcionales para un campo o subcampo, deberá incluirse el número adecuado de carácter separador.

Es posible que existan combinaciones adyacentes de dos o más de los cuatro caracteres separadores disponibles. Cuando los datos para las entradas de información, los subcampos o los campos faltan o no están disponibles, deberá haber un carácter separador menos que el número de entradas de datos, campos o subcampos necesarios.

Cuadro 1: Separadores utilizados

Código	Tipo	Descripción	Valor hexadecimal	Valor decimal
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. *Presentación del registro*

Para los registros lógicos con campos etiquetados, cada uno de los campos de información utilizados se numerará de conformidad con esta norma. El formato de cada campo consistirá en el número del tipo de registro lógico seguido por un punto «.», un número de campo seguido por dos puntos «:», seguido de la información que corresponda a ese campo. El número de campo etiquetado puede ser cualquier cifra de 1 a 9 que figure entre el punto «.» y los dos puntos «:». Se interpretará como un número entero de campo no signado. Esto supone que un número de campo de «2.123:» equivale y deberá interpretarse como un número de campo de «2.000000123:».

A efectos ilustrativos a lo largo de su documento se utilizará un número con tres dígitos para la enumeración de los campos contenidos en cada uno de los registros lógicos de campos etiquetados aquí descritos. Los números de campos tendrán la forma «TT.xxx:»; en la cual «TT» representa el tipo de registro de uno o dos caracteres seguido por un punto. Los tres caracteres siguientes incluyen el número de campo correspondiente seguido por dos puntos. La información descriptiva ASCII o los datos de imagen siguen a los dos puntos.

Los registros lógicos de tipo-1 y tipo-2 solo contienen campos con datos de texto ASCII. La longitud total del registro (incluidos números de campo, dos puntos y caracteres separadores) quedará registrada como el primer campo ASCII dentro de cada uno de estos tipos de registro. El carácter de control separador de archivos ASCII «FS» (indica el fin de un registro lógico o de una transacción) se situará después del último byte de información ASCII y estará incluido en la longitud del registro.

En contraste con el concepto de campo etiquetado, el registro de tipo-4 solo contiene datos binarios registrados como campos binarios de longitud fija ordenados. La longitud completa del registro quedará registrada en el primer campo binario de cuatro bytes de cada registro. Para este registro binario, no se registrarán ni el número de registro con su punto, ni el identificador de campo seguido de sus dos puntos. Además, dado que todas las longitudes de campo de este registro son fijas o están especificadas, ninguno de los cuatro caracteres («US», «RS», «GS» o «FS») se interpretará como algo distinto de los datos binarios. Para el registro binario, el carácter «FS» no se utilizará como separador de registros ni como carácter de determinación de transacciones.

3. ***Registro lógico de tipo-1: Encabezamiento del archivo***

Este registro describe la estructura del archivo, el tipo del archivo así como otros datos importantes. El tipo de caracteres utilizado para los campos de tipo-1 solo contendrá el código ANSI de 7-bit para intercambiar información.

3.1. *Campos para registros lógicos de tipo-1*

3.1.1. Campo 1.001: Longitud del Registro Lógico (LEN)

Este campo contiene el recuento total del número de bytes en la totalidad del registro lógico de tipo-1. El campo comienza por «1.001:», seguido de la longitud total del registro incluidos todos los caracteres de cada uno de los campos y los separadores de información.

3.1.2. Campo 1.002: Número de versión (VER)

Para garantizar que el usuario conozca qué versión de la norma ANSI/NIST se está utilizando, este campo de cuatro bytes especifica el número de versión de la norma utilizada por el programa o el sistema que crea el archivo. Los dos primeros bytes especifican el número de referencia de la versión principal y los dos siguientes, el número de revisión menor. Por ejemplo, la norma original de 1986 se consideraría como la primera versión y se designaría como «0100» mientras que la actual norma ANSI/NIST-ITL 1-2000 se indica como «0300».

3.1.3. Campo 1.003: Contenido de archivo (CNT)

En este campo se enumera cada uno de los registros del archivo clasificados por tipo de registro y según el orden en que aparecen en el archivo lógico. Consiste en uno o varios campos cada uno de los cuales contiene a su vez dos entradas de información que describen un único registro lógico que se encuentra en el archivo actual. Los subcampos se introducen en el mismo orden en que se registran y transmiten los registros.

La primera entrada de información en el primer subcampo es «1», en referencia a este registro de tipo-1. Va seguida de una segunda entrada de información que contiene el número de otros registros que figuran en el archivo. Este número es también igual a la suma de los subcampos restantes del campo 1.003.

Cada uno de los subcampos restantes está asociado con un registro dentro del archivo, y la secuencia de subcampos corresponde a la secuencia de registros. Cada subcampo contiene dos entradas de información. La primera identifica el tipo de registro. La segunda es el IDC del registro. Se utilizará el carácter «US» para separar las dos entradas de información.

3.1.4. Campo 1.004: Tipo de transacción (TOT)

Este campo contiene un código mnemónico de tres letras que designa el tipo de transacción. Estos códigos pueden diferir de los utilizados por otras aplicaciones de la norma ANSI/NIST.

CPS: Búsqueda penal impresión por impresión (Criminal Print-to-Print Search). Esta transacción consiste en una solicitud de búsqueda de un registro relativo a una infracción penal realizando una comparación con una base de datos de impresiones. Las impresiones de la persona deben incluirse en el archivo como imágenes comprimidas WSQ.

En caso de que no se encuentren resultados positivos, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2.

En caso de resultado positivo, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2,

— 1-14 registros de tipo-4.

El tipo de transacción (TOT) CPS se resume en la tabla A.6.1 (apéndice 6).

PMS: Búsqueda de impresión a latente (Print-to-Latent Search). Esta transacción se utiliza cuando una serie de impresiones deben contrastarse con una base de datos de huellas latentes no identificadas. La respuesta contendrá la decisión sobre resultado positivo/ausencia de resultado de la búsqueda de destino AFIS. De existir varias huellas latentes no identificadas, se devolverán varias transacciones SRE, con una latente por transacción. Las impresiones de la persona deben incluirse en el archivo como imágenes comprimidas WSQ.

En caso de que no se encuentren resultados positivos, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2.

En caso de resultado positivo, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2,

— 1 registros de tipo-13.

El tipo de transacción (TOT) PMS se resume en la tabla A.6.1 (apéndice 6).

MPS: Búsqueda de latente a impresión (Latent-to-Print Search). Esta transacción se utiliza cuando una latente debe contrastarse con una base de datos de impresiones. Deberán figurar en el archivo la información sobre puntos característicos de la huella latente y la imagen (comprimida en formato WSQ).

En caso de que no se encuentren resultados positivos, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2.

En caso de resultado positivo, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2,

— 1 registro de tipo-4 o tipo-15.

El tipo de transacción (TOT) MPS se resume en la tabla A.6.4 (apéndice 6).

MMS: Búsqueda de latente a latente. En esta transacción el archivo contiene una latente que debe ser contrastada con una base de datos de huellas latentes no identificadas a fin de establecer vínculos entre varias escenas del crimen. Deberán figurar en el archivo la información sobre puntos característicos de la huella latente y la imagen (comprimida en formato WSQ).

En caso de que no se encuentren resultados positivos, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2.

En caso de resultado positivo, se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2,

— 1 registro de tipo-13.

El tipo de transacción (TOT) MMS se resume en la tabla A.6.4 (apéndice 6).

SRE: Esta transacción es devuelta por el organismo de destino en respuesta a la presentación de datos dactiloscópicos. Esta respuesta contendrá la decisión resultado/sin resultado de la búsqueda de la AFIS de destino. De existir múltiples candidatos, se devolverán varias transacciones SRE, con un candidato por transacción.

El tipo de transacción (TOT) MMS se resume en la tabla A.6.2 (apéndice 6).

ERR: Esa transacción es devuelta por la AFIS de destino para indicar un error de transacción. Incluye un campo de mensaje (ERM) en el que se indica el error detectado. Se devolverán los siguientes registros lógicos:

— 1 registro de tipo-1,

— 1 registro de tipo-2.

El tipo de transacción (TOT) ERR se resume en la tabla A.6.3 (apéndice 6).

Tabla 2: Códigos permitidos para las transacciones

Tipo de transacción	Tipo de registro lógico					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SRE	M	M	C	— (C in case of latent hits)	C	C
MPS	M	M	—	M (1*)	M	—

Tipo de transacción	Tipo de registro lógico					
	1	2	4	9	13	15
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

Clave

M = obligatorio (Mandatory)
M* = solo puede incluirse uno de los tipos de registro
O = optativo
C = condicionado a la disponibilidad de los datos
— = no permitido
1* = condicionado en función de los sistemas de legado

3.1.5. Campo 1.005: Fecha de transacción (DAT)

Este campo indica la fecha en que comenzó la transacción y debe adecuarse a la notación de la norma ISO: YYYYMMDD

YYYY indica el año, MM indica el mes y DD indica el día del mes. Para números de una sola cifra se utilizan ceros de introducción. Por ejemplo, «19931004» representa el 4 de octubre de 1993.

3.1.6. Campo 1.006: Prioridad (PRY)

Este campo opcional define la prioridad de la solicitud, en una escala de 1 a 9. «1» representa la máxima prioridad y «9» la más baja. Las transacciones de prioridad «1» se tramitarán de inmediato.

3.1.7. Campo 1.007: Identificador de la Agencia de Destino (Destination Agency Identifier) (DAI)

Este campo especifica la agencia de destino de la transacción.

Está compuesto de dos entradas de información en el siguiente formato: CC/agencia.

La primera entrada de información contiene el código de país definido en ISO 3166, compuesto de dos caracteres alfanuméricos. La segunda entrada, *agencia*, es una identificación de texto libre de la agencia con un máximo de 32 caracteres alfanuméricos.

3.1.8. Campo 1.008: Identificador de la Agencia de Origen (ORI)

Este campo especifica el origen del archivo y tiene el mismo formato que DAI (campo 1.007).

3.1.9. Campo 1.009: Número de Control de Transacción (Transaction Control Number) (TCN)

Se trata de un número de control a efectos de referencia. Debería generarlo el ordenador con el siguiente formato: YYSSSSSSSSA.

YY es el año de la transacción, SSSSSSSS es un número de serie de ocho dígitos, y A es un carácter de control generado mediante el procedimiento que figura en el apéndice 2.

Cuando no se disponga de TCN, el campo YYSSSSSSSS se rellena con ceros y con el carácter de control antes mencionado.

3.1.10. Campo 1.010: Respuesta de control de transacción (Transaction Control Response) (TCR)

Cuando se remite una solicitud cuya respuesta es esta, este campo opcional contendrá el número de control de la transacción del mensaje de solicitud. Tiene por consiguiente el mismo formato que TCN (campo 1.009).

3.1.11. Campo 1.011: Resolución del escaneo de origen (Native Scanning Resolution) (NSR)

Este campo especifica la resolución normal del barrido del sistema utilizado por el iniciador de la transacción. La resolución se especifica en forma de dos dígitos numéricos seguidos de un punto decimal y de otros dos dígitos.

Para todas las transacciones correspondientes a la Decisión 2008/615/JAI la proporción de muestreo será de 500 pixels/pulgada o 19,68 pixels/mm.

3.1.12. Campo 1.012: Resolución nominal de transmisión (Nominal Transmitting Resolution) (NTR)

Este campo de cinco bytes especifica la resolución nominal de transmisión de las imágenes transmitidas. La resolución se expresa en pixels/mm en el mismo formato que NSR (campo 1.011).

3.1.13. Campo 1.013: Nombre de Dominio (Domain name) (DOM)

Este campo obligatorio identifica el nombre de dominio para la aplicación del registro lógico de tipo-2 definido por el usuario. Contiene dos entradas de información y será «INT-I{US}4.22{GS}».

3.1.14. Campo 1.014: Hora del meridiano de Greenwich (Greenwich mean time) (GMT)

Este campo obligatorio proporciona un mecanismo para expresar la fecha y la hora en términos de unidades de hora del meridiano de Greenwich (GMT). Si se utiliza, el campo GMT contiene la fecha universal que se añadirá a la fecha local que figura en el campo 1.005 (DAT). El uso del campo GMT suprime las incoherencias entre horarios locales que se dan cuando una transacción y su respuesta se transmiten entre los lugares separados por varias zonas horarias. El GMT proporciona una fecha universal y un reloj de 24 horas independiente de las zonas horarias. Se representa como «CCYYMMDDHHMMSSZ», una serie de 15 caracteres consistente en la concatenación de la fecha con la hora GMT y terminada por una «Z». Los caracteres «CCYY» representarán el año de la transacción, los caracteres «MM» corresponderán a los valores de decenas y de unidades del mes, y los caracteres «DD» corresponderán a los valores de decenas y unidades del día del mes, los caracteres «HH» representan la hora, «MM» el minuto, y «SS» el segundo. La fecha completa no superará la fecha corriente.

4. ***Registro lógico de tipo-2: Texto descriptivo***

La estructura de la mayor parte de este registro no está definida por la norma originaria ANSI/NIST. El registro contiene información de interés específico para las agencias que remiten o reciben el archivo. Para garantizar que los sistemas dactiloscópicos en comunicación sean compatibles, es necesario que solo figuren en el registro los campos enumerados más abajo. El presente documento especifica qué campos son obligatorios y cuáles opcionales, y también define la estructura de cada uno de los campos.

4.1. *Campos para registros lógicos de tipo-2*

4.1.1. Campo 2.001: Longitud del registro lógico (Logical Record Length) (LEN)

Este campo obligatorio contiene la longitud de este registro de tipo-2, y especifica el número total de bytes con inclusión de cada uno de los caracteres de cada campo que figura en el registro así como de los separadores de información.

4.1.2. Campo 2.002: Carácter de designación de imagen (Image Designation Character) (IDC)

El IDC que figura en este campo obligatorio es una representación ASCII del IDC tal como se define en el campo de contenidos del archivo (CNT) del registro de tipo-1 (campo 1.003).

4.1.3. Campo 2.003: Información sobre el sistema (System Information) (SYS)

Este campo es obligatorio y contiene cuatro bytes que indican a qué versión de INT-I corresponde este tipo particular de registro de tipo-2.

Los dos primeros bytes especifican el número de la versión principal, los dos segundos el número de la revisión menor. Por ejemplo, esta aplicación se basa en INT-I versión 4 revisión 22, lo que se representaría como «0422».

4.1.4. Campo 2.007: Número de asunto (Case Number) (CNO)

Se trata de un número atribuido por la oficina dactiloscópica local a una colección de huellas latentes encontrada en la escena del crimen. Se adopta el siguiente formato: CC/number.

CC es el código de país de Interpol, con una longitud de dos caracteres alfanuméricos, y el «número» corresponde a las directrices locales correspondientes y puede tener una longitud de hasta 32 caracteres alfanuméricos.

Este campo permite al sistema identificar las huellas latentes asociadas con un delito particular.

4.1.5. Campo 2.008: Número de secuencia (Sequence Number) (SQN)

Este campo especifica cada secuencia de huellas latentes dentro de un caso. Puede llegar a una longitud de hasta cuatro caracteres numéricos. Una secuencia es una huella latente o una serie de huellas latentes agrupadas a efectos de archivado o de búsqueda. Esa definición supone que tendrá que asignarse un número de secuencia incluso a las huellas latentes únicas.

Podrá incluirse este campo, junto con MID (campo 2.009) para identificar una latente particular dentro de una secuencia.

4.1.6. Campo 2.009: Identificador de huella latente (Latent Identifier) (MID)

Este campo especifica la huella latente individual dentro de una secuencia. El valor es una única letra o dos letras, asignándose la «A» a la primera latente, la «B» al segundo y así sucesivamente hasta un límite de «ZZ». Este campo se utiliza de manera análoga al número de secuencia latente a que se refiere la descripción de SQN (campo 2.008).

4.1.7. Campo 2.010: Número de identificación personal (Criminal Reference Number) (CRN)

Se trata de un número de referencia único asignado por una agencia nacional a un individuo acusado por primera vez de haber cometido un delito. Dentro de un solo país ningún individuo tendrá más de un CRN, ni lo compartirá con ningún otro individuo. No obstante, un mismo individuo podrá tener varios números de referencia criminal en varios países que podrán distinguirse por medio del código de país.

Se adopta el siguiente formato para el campo CRN: CC/number.

CC es el código del país, definido en ISO 3166, de dos caracteres alfanuméricos de longitud, y el «número» corresponde a las directrices nacionales correspondientes de la agencia emisora y podrá tener una longitud de hasta 32 caracteres alfanuméricos.

Para las transacciones efectuadas con arreglo a la Decisión 2008/615/JAI ese campo se utilizará para el Número de identificación personal nacional de la agencia de origen que estará conectado con las imágenes de los registros de tipo-4 o tipo-15.

4.1.8. Campo 2.012: Distintos números de referencia (Miscellaneous Identification Number) (MN1)

Estos campos contienen el CRN (campo 2.010) transmitido por una transacción CPS o PMS sin el número de país líder.

4.1.9. Campo 2.013: Distintos números de referencia (Miscellaneous Identification Number) (MN2)

Estos campos contienen el CNO (campo 2.007) transmitido por una transacción MPS o MMS sin el número de país líder.

4.1.10. Campo 2.014: Distintos números de referencia (Miscellaneous Identification Number) (MN3)

Estos campos contienen el SQN (campo 2.008) transmitido por una transacción MPS o MMS.

4.1.11. Campo 2.015: Distintos números de referencia (Miscellaneous Identification Number) (MN4)

Estos campos contienen el MID (campo 2.009) transmitido por una transacción MPS o MMS.

4.1.12. Campo 2.063: Información adicional (Additional Information) (INF)

En caso de una transacción SRE para una solicitud PMS, este campo da información sobre el dedo que dio lugar al posible RESULTADO. El formato del campo es:

NN siendo *NN* el código de posición del dedo definido en la tabla 5, con una longitud de dos dígitos.

En todos los demás casos este campo es opcional. Consiste en un máximo de 32 caracteres alfanuméricos y puede dar información adicional sobre la solicitud.

4.1.13. Campo 2.064: Lista de posibles respuestas (Respondents List RLS)

Este campo contiene como mínimo dos campos. El primero describe el tipo de búsqueda que se ha llevado a cabo utilizando los códigos mnemónicos de tres letras que especifica el tipo de transacción en TOT (campo 1.004). El segundo campo contiene un único carácter. Se utilizará una «I» para indicar que se ha encontrado un RESULTADO POSITIVO y una «N» para indicar que no se han encontrado casos coincidentes (SIN RESULTADO). El tercer campo contiene el identificador de secuencia para el resultado candidato y el número total de candidatos separados por una barra. Se devolverán varios mensajes si existen varios candidatos.

En caso de un posible RESULTADO POSITIVO el cuarto campo contendrá un valor con una longitud máxima de seis dígitos. Si se ha comprobado el RESULTADO POSITIVO el valor de este subcampo se decidirá como «999999».

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

Si el AFIS remoto no atribuye valores, se utilizará un valor cero en el punto correspondiente.

4.1.14. Campo 2.074: Campo de mensaje de estado/error (Status/Error Message) (ERM)

Este campo contiene mensajes de error resultantes de las transacciones, que se devolverán al solicitante en el marco de una transacción de error.

Cuadro 3: Mensajes de error

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.

Mensajes de error con valores comprendidos entre 100 y 199:

Estos mensajes de error están relacionados con la validación de los registros ANSI/NIST y se definen del siguiente modo:

<código_error 1>: IDC <número_idc 1> FIELD <id_campo 1> <texto dinámico 1> LF

<código_error 2>: IDC <número_idc 2> FIELD <id_campo 2> <texto dinámico 2>…

donde:

— código_error es un código vinculado a un único motivo específico (véase el cuadro 3),

— id_campo es el número de campo ANSI/NIST del campo incorrecto (por ejemplo, 1.001, 2.001, …) en el formato <tipo_registro>.id_campo>.id_sub_campo>,

— texto dinámico es una descripción dinámica y más detallada del error,

— LF (Line Feed) significa salto de línea y separa cada error en el caso de que se produzca más de uno,

— para el registro de tipo-1 el ICD se define como «-1».

Ejemplo:

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

Este campo es obligatorio para transacciones de error.

4.1.15. Campo 2.320: Número previsto de candidatos (Expected Number of Candidates) (ENC)

Este campo contiene el número máximo de candidatos a la verificación previsto por el organismo solicitante. El valor de ENC no debe exceder los valores definidos en el cuadro 11.

5. ***Registro de tipo-4: Imagen de alta resolución en escala de grises***

Cabe señalar que las fichas de tipo-4 son binarias y no de tipo ASCII. Por lo tanto se ha asignado a cada campo una posición específica dentro del registro, lo cual implica que todos los campos son obligatorios.

La norma permite precisar en el registro tanto el tamaño como la resolución de la imagen. Los datos de las imágenes dactiloscópicas que aparecen en estos registros se deben enviar con una densidad de entre 500 y 520 píxeles por pulgada. Para la creación de imágenes se recomienda usar 500 píxel por pulgada, o 19,68 píxeles/mm. En la INT-I se especifica que la densidad deberá ser de 500 píxeles por pulgada, pero dos sistemas similares pueden utilizar para sus intercambios otra resolución comprendida entre 500 y 520 píxeles por pulgada.

5.1. *Campos del registro de tipo-4*

5.1.1. Campo 4.001: Longitud del registro lógico (Logical Record Length) (LEN)

En este campo de cuatro bytes se indica la longitud de este registro de tipo-4 y la cantidad total de bytes, así como el número de bytes en cada uno de los campos del registro.

5.1.2. Campo 4.002: Carácter de designación de la imagen (Image Designation Character) (IDC)

Se trata de un byte con la representación binaria del número que aparece en el fichero de encabezamiento.

5.1.3. Campo 4.003: Tipo de impresión (Impression Type) (IMP)

Es un campo de un solo byte, que ocupa el sexto byte del registro.

Cuadro 4: Tipo de impresión dactilar

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

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

5.1.4. Campo 4.004: Posición del dedo (Finger Position) (FGP)

Este campo, de una longitud fija de seis bytes, ocupa los bytes 7 al 12 del registro de tipo-4. En él figuran las posibles posiciones del dedo a partir del byte que se encuentra más a la izquierda (byte 7 del registro). La posición del dedo conocida o más probable se define en función del cuadro que figura al final del presente párrafo. Se pueden añadir otras cinco referencias introduciendo las posiciones alternativas del dedo en los cinco bytes restantes, siguiendo el mismo formato. Si se utilizan menos de cinco referencias de posición de dedo, los bytes que no se empleen llevarán el valor 255 en binario. Cuando no se sepa la posición del dedo se indicará el valor 0 (dedo desconocido).

Cuadro 5: Código de posición y tamaño máximo del dedo

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 las huellas latentes solo se utilizarán los códigos 0 a 10.

5.1.5. Campo 4.005: Resolución de escaneado de la imagen (Image Scanning Resolution-ISR)

Este campo, de un solo byte, ocupa el byte 13 del registro de tipo-4. Si en él figura «0», la imagen ha sido escaneada con la resolución recomendada (19,68 píxeles/mm o 500 píxeles por pulgada), y si figura «1», ha sido escaneada con otra resolución, como se indica en el registro de tipo-1.

5.1.6. Campo 4.006: Longitud de línea horizontal (Horizontal Line Length) (HLL)

Este campo ocupa los bytes 14 y 15 del registro de tipo-4. En él se especifica el número de píxeles que hay en cada línea escaneada. El primer byte es el más importante.

5.1.7. Campo 4.007: Longitud de línea vertical (Vertical Line Length) (VLL)

Este campo ocupa los bytes 16 y 17 del registro de tipo-4; en él se especifica la cantidad de líneas que aparecen en la imagen escaneada. El primer byte es el más importante.

5.1.8. Campo 4.008: Algoritmo de compresión en escala de grises (Greyscale Compression Algorithm) (GCA)

En este campo de un byte se especifica el algoritmo de compresión de escala de grises que se ha utilizado para codificar los datos de la imagen. Para esta aplicación, un código binario 1 indica que se ha utilizado una compresión WSQ (apéndice 7).

5.1.9. Campo 4.009: Imagen

En este campo figura una serie de bytes que representa a la imagen. Su estructura dependerá evidentemente del algoritmo de compresión que se haya utilizado.

6. ***Registro de tipo-9: Puntos característicos***

En los registros de tipo-9 debe figurar un texto de tipo ASCII en el que se describan los puntos característicos y otros datos cifrados de huellas latentes. En el caso de una transacción de búsqueda de latentes, no hay limitación para estos registros de tipo-9 en un fichero, y cada uno de ellos corresponderá a una vista o latentes diferentes.

6.1. *Obtención de puntos característicos*

6.1.1. Identificación de los tipos de puntos característicos

Esta norma permite definir tres caracteres de identificación que se utilizan para describir los distintos tipos de puntos característicos (véase el cuadro 6). El extremo de una cresta será designado tipo-1. Una bifurcación será designada tipo-2. Si un punto característico no corresponde claramente a uno de los tipos descritos, será designado «otro», es decir tipo-0.

Cuadro 6: Tipos de puntos característicos

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Situación y tipo de los puntos característicos

Para que las plantillas se ajusten a lo dispuesto en la sección 5 de la norma ANSI INCITS 378-2004, se aplicará el método siguiente, que mejora la actual norma INCITS 378-2004, para determinar la situación (punto y dirección angular) de los puntos característicos individuales.

La posición o situación de un punto característico que representa el extremo de una cresta será el punto de bifurcación del esqueleto central del valle inmediatamente anterior al extremo de la cresta. Si las tres ramas del valle se redujeran a un esqueleto de un solo píxel de ancho, el punto característico se situaría en la intersección de las tres ramas. Del mismo modo, la situación del punto característico correspondiente a una bifurcación será el punto de bifurcación del esqueleto central de la cresta. Si se redujeran las tres ramas de la cresta a un esqueleto de un solo píxel de ancho, el punto característico se situaría en la intersección de los tres brazos.

Después de que todos los extremos de las crestas se hayan convertido en bifurcaciones, todos los puntos característicos de la imagen dactiloscópica se representan como bifurcaciones. Las coordenadas de un píxel de X e Y de la intersección de las tres ramas de cada punto característico pueden formatearse directamente. La determinación de la dirección del punto característico puede extraerse de cada bifurcación del esqueleto. Las tres ramas de cada bifurcación del esqueleto deben examinarse y debe determinarse el final de cada brazo. El cuadro 6.1.2 ilustra los tres métodos utilizados para determinar el final de una rama que está basada en una resolución de escaneado de 500 píxeles por pulgada.

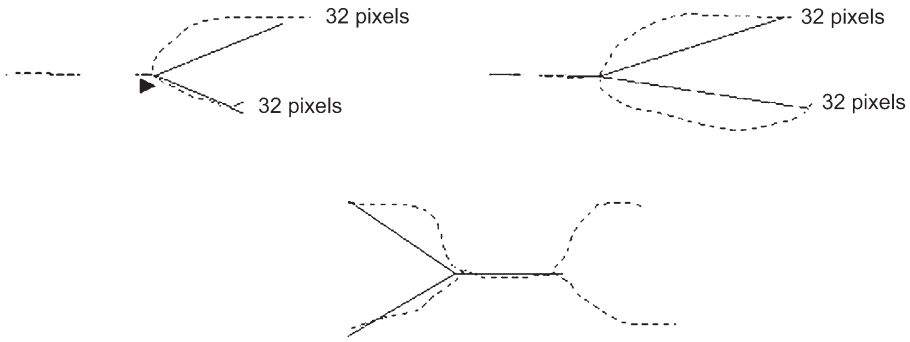
El final se establece en función de lo que ocurra primero. La densidad de píxeles se basa en una resolución de escaneado de 500 píxeles por pulgada. Resoluciones de escaneado distintas producirían densidades de píxeles distintas.

— una distancia de .064" (el 32° píxel),

— el final de la rama del esqueleto que aparezca entre una distancia de .02" y .064" (el 10° de los 32 píxeles); las ramas más cortas no se tienen en cuenta,

— se encuentra una segunda bifurcación en una distancia de .064" (antes del 32° píxel).

Figura 6.1.2



El ángulo de los puntos característicos se determina trazando tres rayos virtuales con origen en el punto de bifurcación y que se extienden hasta el extremo de cada rama. El más pequeño de los tres ángulos formados por los rayos se biseca para indicar la dirección de los puntos característicos.

6.1.3. Sistema de coordenadas

El sistema de coordenadas utilizado para expresar los puntos característicos de una huella dactilar será un sistema de coordenadas cartesianas. La situación de los puntos característicos se representará mediante sus coordenadas X e Y. El origen del sistema de coordenadas será la esquina superior izquierda de la imagen original, de forma que X aumentará hacia la derecha e Y aumentará hacia abajo. Las coordenadas X e Y de los puntos característicos se representarán ambas en unidades de píxel a partir del origen. Cabe señalar que la situación del origen y las unidades de medida no concuerdan con la convención seguida en las definiciones de tipo-9 de la norma ANSI/NIST-ITL 1-2000.

6.1.4. Dirección de los puntos característicos

Los ángulos se expresan en el formato matemático estándar, con cero grados a la derecha y los ángulos que aumentan en sentido inverso a las agujas del reloj. Los ángulos registrados van en dirección hacia atrás a lo largo de la cresta respecto del final de una cresta y hacia el centro del valle en el caso de una bifurcación. Esta convención presenta una oposición de 180 grados respecto de la convención para ángulos descrita en las definiciones del tipo-9 de la norma ANSI/NIST ITL 1-2000.

6.2. *Campos del registro de tipo-9 en formato INCITS-378*

Todos los campos de los registros de tipo-9 deben de introducirse como un texto ASCII. En este registro de campos identificados no pueden introducirse campos binarios.

6.2.1. Campo 9.001: Longitud del registro lógico (Logical record length) (LEN)

Este campo ASCII obligatorio debe contener la longitud del registro que especifica el número total de bytes, incluidos todos y cada uno de los caracteres de cada campo comprendido en el registro.

6.2.2. Campo 9.002: Carácter de designación de la imagen (Image designation character) (IDC)

Este campo obligatorio de dos bytes deberá emplearse para la identificación y localización de los puntos característicos. El IDC de este campo debe ser idéntico al IDC que aparece en el campo de contenido de archivo del registro de tipo-1

6.2.3. Campo 9.003: Tipo de impresión (Impression type) (IMP)

Este campo obligatorio de un byte describirá cómo se obtuvo la información de la imagen dactiloscópica. Se debe introducir en este campo el valor ASCII del código que corresponda entre los que figuran en el cuadro 4.

6.2.4. Campo 9.004: Formato de los puntos característicos (Minutiæ format) (FMT)

Este campo contendrá una «U» para indicar que los puntos característicos están formateados según la norma M1-378. Aun cuando la información se codifique según la norma M1-378, todos los campos de datos del registro de tipo-9 deben seguir siendo campos de texto ASCII.

6.2.5. Campo 9.126: Información CBEFF

Este campo contendrá tres elementos de información. El primero contendrá el valor «27» (0x1B). Esta es la identificación del propietario del formato CBEFF asignada por la Asociación internacional de la industria biométrica (IBIA) al Comité técnico M1 INCITS. El carácter <US> delimitará este punto del tipo de formato CBEFF al que se asigna un valor de «513» (0x0201) a fin de indicar que este documento contiene solamente la situación y

datos de dirección angular sin ninguna información en el bloque de datos extenso. El carácter <US> delimitará este punto del identificador del producto (PID) CBEFF, que identifica al «propietario» del equipo de codificación. El proveedor establece este valor. Puede obtenerse en el sitio Internet de la IBIA (www.ibia.org) si ha sido incluido en la lista que aparece en dicho sitio.

6.2.6. Campo 9.127: Identificación de equipo de escaneado de la imagen

Este campo contendrá dos elementos de información separados por el carácter <US>. El primero contendrá «APPF» si se certificara que el equipo utilizado originalmente para escanear la imagen cumple con el apéndice F [especificación de la calidad de la imagen del IAFIS (Integrated Automated Fingerprint Identification System), 29 de enero de 1999] de CJIS-RS-0010, la norma para la transmisión electrónica de huellas dactilares del Federal Bureau of Investigation (FBI). Si el equipo no se ajustara a la citada norma contendrá el valor de «NINGUNO». El segundo elemento de información contendrá la identificación del equipo de escaneado, que es un número de producto asignado por el proveedor del equipo de escaneado. Un valor de «0» indica que no se dispone de la identificación del equipo.

6.2.7. Campo 9.128: Longitud de línea horizontal (Horizontal line length) (HLL)

Este campo obligatorio del ASCII contendrá el número de píxeles contenidos en una sola línea horizontal de la imagen transmitida. El tamaño horizontal máximo está limitado a 65 534 píxeles.

6.2.8. Campo 9.129: Longitud de línea vertical (Vertical line length) (VLL)

Este campo obligatorio del ASCII contendrá el número de líneas horizontales contenidas en la imagen transmitida. El tamaño vertical máximo está limitado a 65 534 píxeles.

6.2.9. Campo 9.130: Unidades de medida (SLC)

Este campo ASCII obligatorio indicará las unidades empleadas para describir la densidad de píxeles de la imagen. Se empleará el «1» para indicar los píxeles por pulgada y el «2» si se trata de píxeles por centímetros. Si aparece un «0» no se proporciona la escala. En este caso la proporción se obtendrá dividiendo la HPS (escala horizontal de píxel) por la VPS.

6.2.10. Campo 9.131: Escala horizontal de píxel (Horizontal pixel scale) (HPS)

Este campo ASCII obligatorio indica en números enteros la densidad de píxeles de las líneas horizontales siempre y cuando en el campo SLC se haya expresado la unidad de medida con un «1» o un «2», en caso contrario indica el número de píxeles del componente horizontal.

6.2.11. Campo 9.132: Escala vertical de píxel (Vertical pixel scale) (VPS)

Este campo ASCII obligatorio indica en números enteros la densidad de píxel de las líneas verticales siempre y cuando en el campo SLC se haya expresado la unidad de medida con un «1» o un «2», en caso contrario indica el número de píxeles del componente vertical.

6.2.12. Campo 9.133: Vista del dedo

Este campo obligatorio indica el número de vista del dedo asociado a este dato del registro. El número de vista comienza con «0» y aumenta de uno en uno hasta «15».

6.2.13. Campo 9.134: Posición del dedo (Finger position) (FGP)

Este campo indica el código que designa la posición del dedo que produjo la información de este documento de tipo-9. Se empleará un código entre 1 y 10 tomado del cuadro 5 o el código de palma apropiado del cuadro 10 para indicar la posición del dedo o la palma.

6.2.14. Campo 9.135: Calidad del dedo

El campo indica la calidad de los datos globales sobre los puntos característicos del dedo y estará entre 0 y 100. Este número es una expresión global de la calidad del registro del dedo, y representa la calidad de la imagen original, de la obtención de los puntos característicos y de cualquier operación adicional que pueda afectar al documento de puntos característicos.

6.2.15. Campo 9.136: Número de puntos característicos

El campo obligatorio indica el número de puntos característicos que figuran en este registro.

6.2.16. Campo 9.137: Datos referentes a los puntos característicos del dedo

Este campo obligatorio contiene seis elementos de información separados por el carácter <US>. Consiste en varios subcampos, cada uno de los cuales contiene los detalles de puntos característicos individuales. El número total de subcampos de los puntos característicos debe coincidir con el que figura en el campo 136. El primer elemento de información es el número de puntos característicos del índice, que comenzará por «1» y se incrementará en «1» para cada punto característico adicional de la impresión dactilar. El segundo y el tercer elemento de información son las coordenadas X e Y de los puntos característicos en unidades de píxel. El cuarto elemento de información es el ángulo de los puntos característicos registrado en unidades de dos grados. Este valor será no negativo entre 0 y 179. El quinto elemento de información es el tipo de punto característico. Se usa un valor de «0» para representar puntos característicos del tipo «OTRO», un valor de «1» para el extremo de una cresta y un valor de «2» para la bifurcación de una cresta. El sexto elemento de información representa la calidad de cada punto característico. Este valor estará comprendido entre un mínimo de 1 y un máximo de 100. El valor «0» indica que no se dispone de ningún valor relativo a la calidad. Cada subcampo se separará del siguiente por medio del carácter de separación <RS>.

6.2.17. Campo 9.138: Información sobre el recuento de crestas

Este campo consiste en una serie de subcampos de los cuales cada uno contiene tres elementos de información. El primer elemento de información del primer subcampo indica el método de recuento del número de crestas. Un «0» indica que no se hará ninguna suposición sobre el método utilizado para obtener el número de crestas, ni su orden en el documento. Un «1» indica que para cada punto característico central, el recuento de las crestas se ha hecho hasta el punto característico contiguo más próximo en cuatro cuadrantes, y los recuentos de crestas correspondientes a cada punto característico central se indican juntos. Un «2» indica que para punto característico central, el recuento de crestas se ha efectuado hasta los puntos característicos contiguos más próximos en ocho octantes, y los recuentos de crestas correspondientes a cada punto característico central se indican juntos. Los dos elementos de información restantes del primer subcampo contendrán ambos un «0». Los elementos de información irán separados por el carácter de separación <US>. Los subcampos siguientes contendrán el número de índice de los puntos característicos centrales como primer elemento de información, el número de índice de los puntos característicos contiguos como segundo elemento de información, y el número de crestas cruzadas como tercer elemento de información. Los subcampos irán separados por el carácter de separación <RS>.

6.2.18. Campo 9.139: Información sobre el centro

Este campo se compondrá de un subcampo por cada centro que haya en la imagen original. Cada subcampo contendrá tres elementos de información. Los dos primeros elementos contendrán las coordenadas de posición X e Y en unidades de píxel. El tercer elemento de información contendrá el ángulo del centro registrado en unidades de dos grados. El valor será un valor no negativo comprendido entre 0 y 179, y los centros múltiples irán separados por el carácter de separación <RS>.

6.2.19. Campo 9.140: Información sobre los deltas

Este campo consistirá en un subcampo para cada delta que aparezca en la imagen original. Cada subcampo contendrá tres elementos de información. Los dos primeros elementos contendrán las coordenadas de posición X e Y en unidades de píxel. El tercer elemento de información contendrá el ángulo del delta registrado en unidades de dos grados. El valor será un valor no negativo entre 0 y 179, y los centros múltiples serán separados por el carácter de separación <RS>.

7. ***Registro de tipo-13 de resolución variable de imagen de huella latente***

El registro de tipo-13 con campos identificados contendrá datos de imagen obtenidos de imágenes latentes. Estas imágenes deben en principio transmitirse a los organismos que obtendrán información automáticamente o las someterán a intervención y tratamiento humanos para extraer la información de característica deseada de las imágenes.

La información relativa a la resolución de escaneado utilizada, al tamaño de imagen, y a otros parámetros requeridos para tratar la imagen, se incluye en el registro en forma de campos identificados.

Cuadro 7: Presentación de los registros de tipo-13, de resolución variable de huellas latentes

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13 001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13 002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13 003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13 004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
LCD	M	13 005	LATENT CAPTURE DATE	N	9	9	1	1	16

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
HLL	M	13 006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	13 007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13 008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13 009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13 010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13 011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	13 012	bits PER PIXEL	N	2	3	1	1	10
FGP	M	13 013	FINGER POSITION	N	2	3	1	6	25
RSV		13 014 13 019	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
COM	O	13 020	COMMENT	A	2	128	0	1	135
RSV		13 021 13 199	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
UDF	O	13 200 13 998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	13 999	IMAGE DATA	B	2	—	1	1	—

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

7.1. *Campos de los registros de tipo-13*

A continuación se describen los datos que contiene cada uno de los campos del registro de tipo-13.

En un registro de tipo-13, las entradas deben figurar en campos numerados. Los dos primeros campos del registro han de respetar un orden y el último campo debe contener la imagen. En el cuadro 7 se indica la condición del campo —obligatorio («O») o facultativo («F»)—, su número, su nombre, el tipo de caracteres empleado, la longitud del campo y el número de veces que puede aparecer. Teniendo en cuenta un número de campo de tres cifras, en la última columna se señala el número máximo de bytes que puede contener. Si se emplean más cifras para el número de campo, el número máximo de bytes aumentará. En las dos entradas de tamaño de campo se cuentan todos los caracteres de separación empleados en el campo. El máximo de bytes comprende el número de campo, la información y los caracteres de separación, incluido el carácter «GS».

7.1.1. Campo 13.001: Longitud del registro lógico (Logical record length) (LEN)

Este campo ASCII obligatorio recoge el cómputo total de bytes del registro de tipo-13. El campo 13.001 debe especificar la longitud del registro incluyendo todos los caracteres de cada campo del registro y los caracteres de separación.

7.1.2. Campo 13.002: Carácter de designación de imagen (Image designation character) (IDC)

Este campo ASCII obligatorio deberá emplearse para identificar la imagen de huella latente que contiene el registro. Este IDC coincidirá con el IDC que figure en el campo (CNT) de contenido de archivo del registro de tipo-1.

7.1.3. Campo 13.003: Tipo de impresión (Impression type) (IMP)

Este campo ASCII obligatorio de uno o dos bytes indicará el modo de obtención de la huella latente. Habrá de introducirse aquí el código apropiado de entre los que figuran en el cuadro 4 (huella dactilar) o en el cuadro 9 (huella palmar).

7.1.4. Campo 13 004: Organismo de origen/ORI (Source agency) (SRC)

Este campo ASCII obligatorio contiene la identificación de la administración u organización que obtuvo inicialmente la huella latente contenida en el registro. En general, habrá de indicarse aquí el ORI del organismo que tomó la huella. Se compone de dos elementos de información con el siguiente formato: CP/organismo.

El primer elemento de información contiene el código de país de Interpol y tiene una longitud de dos caracteres alfanuméricos. El segundo, organismo, es un campo de texto libre de un máximo de 32 caracteres alfanuméricos, que identifica al organismo.

7.1.5. Campo 13.005: Fecha de obtención de la huella latente (Latent capture date) (LCD)

Esta campo ASCII obligatorio indicará la fecha en la que se tomó la huella latente contenida en el registro. La fecha se expresará en el formato de ocho dígitos siguiente: CCYYMMDD. En donde CCYY representa el año en que se tomó la imagen, MM el mes en unidades y decenas y DD las decenas y unidades correspondientes al día del mes. Así, por ejemplo, 20000229 representa el 29 de febrero de 2000. La fecha completa debe ser una fecha real.

7.1.6. Campo 13.006: Longitud de línea horizontal (Horizontal line length) (HLL)

Este campo ASCII obligatorio indica el número de píxeles en cada línea horizontal de la imagen transmitida.

7.1.7. Campo 13.007: Longitud de línea vertical (Vertical line length) (VLL)

Este campo ASCII obligatorio indica el número de líneas horizontales de la imagen transmitida.

7.1.8. Campo 13.008: Unidades de medida (Scale units) (SLC)

Este campo ASCII obligatorio indicará las unidades empleadas para describir la densidad de píxeles. Se empleará el «1» si se trata de píxeles por pulgada y el «2» si se trata de píxeles por centímetros. Si aparece un «0» no se proporciona la escala. En este caso la proporción de píxeles se obtendrá dividiendo la HPS por la VPS.

7.1.9. Campo 13.009: Escala horizontal de píxel (Horizontal pixel scale) (HPS)

Este campo ASCII obligatorio indica en números enteros la densidad de píxeles de las líneas horizontales siempre y cuando en el campo SLC se haya expresado la unidad de medida con un «1» o un «2», en caso contrario indica la cantidad de píxeles de componente horizontal.

7.1.10. Campo 13.010: Escala vertical de píxel (Vertical pixel scale) (VPS)

Este campo ASCII obligatorio indica en números enteros la densidad de píxeles de las líneas verticales siempre y cuando en el campo precedente SLC se haya expresado la unidad de medida con un «1» o un «2», en caso contrario indica el número de píxeles del componente vertical.

7.1.11. Campo 13.011: Algoritmo de compresión (Compression algorithm) (CGA)

Este campo ASCII obligatorio especificará el algoritmo utilizado para comprimir las imágenes en escala de grises. Véase el apéndice 7 para los códigos de compresión.

7.1.12. Campo 13.012: Bits por píxel (Bits per pixel) (BPX)

Este campo ASCII obligatorio ha de contener el número de bits utilizados para representar un píxel. Este campo aparecerá marcado con un «8» para indicar unos valores normales de escala de grises comprendidos entre el «0» y el «255». Un número por encima de «8» indicará que el píxel de escala de grises tiene una precisión mayor.

7.1.13. Campo 13.013: Posición del dedo o de la palma (Finger/palm position) (FGP)

Este campo identificado obligatorio indica una o varias posiciones posibles del dedo o la palma que podría corresponder a la de la huella latente. El código de número decimal correspondiente a la posición del dedo conocida o más probable figura en el cuadro 5, y el de la posición palmar más probable en el cuadro 10. Este código se introducirá como un subcampo ASCII de uno o dos caracteres. Si hubiera que añadir otras posiciones dactilares o palmares se añadirían los códigos correspondientes como subcampos separados por el carácter «RS». El código «0» (dedo desconocido) se utilizará para cualquier posición del 1 al 10. El código «20» (palma desconocida) se empleará para cualquier posición palmar que figure en la lista.

7.1.14. Campos 13.014-019: Reservados para introducir datos en el futuro (RSV)

Estos campos se reservan para futuras revisiones de esta norma. Por el momento estos campos no deben emplearse. En caso de que aparezcan, se deberá hacer caso omiso de ellos.

7.1.15. Campo 13.020: Comentarios (Comment) (COM)

Este campo opcional puede utilizarse para hacer observaciones o añadir información en forma de texto ASCII con la imagen de huella latente.

7.1.16. Campos 13.021-199: Reservado para introducir datos en el futuro (Reserved for future definition) (RSV)

Estos campos se reservan para añadir futuras revisiones de esta norma. De momento no deben emplearse. En caso de que aparezcan, se deberá hacer caso omiso de ellos.

7.1.17. Campos 13.200-998: Campos definidos por el usuario (User-defined fields) (UDF)

Estos campos son definidos por el usuario y se utilizarán para requisitos futuros. Su tamaño y contenido serán definidos por el usuario y de conformidad con el organismo de recepción. Si aparecen contendrán información textual ASCII.

7.1.18. Campo 13.999: Imagen (Image data) (DAT)

Este campo contiene la imagen de la huella latente. Siempre tendrá el número 999 y será el último campo del registro. Así por ejemplo, «13.999:» va seguido de una representación binaria de la imagen.

Cada píxel de una escala de grises sin comprimir se limitará normalmente a ocho bits (256 tonos de grises) dentro de un único byte. Si en el campo BPX, 13.012, se introdujo un número inferior o superior a «8», el número de bytes necesarios para cada píxel será diferente. Si se lleva a cabo la compresión, los píxeles habrán de comprimirse utilizando la técnica que se determine en el campo GCA.

7.2. *Fin del registro de tipo-13 de imagen de huella latente de resolución variable*

La lógica del sistema requiere que al final del último dato del campo 13.999 aparezca un separador «FS» indicando el final de este registro, antes de comenzar uno nuevo. Este separador debe contarse en el campo de longitud del registro de tipo-13.

8. ***Registro de tipo-15 de imagen de impresión palmar de resolución variable***

El registro de campo identificado de tipo-15 tendrá datos sobre imágenes de impresiones palmares y los textos, fijos y definidos por el usuario, que acompañan la imagen digitalizada. La información sobre la resolución utilizada, el tamaño de la imagen y otros parámetros o información pertinente para el tratamiento de la imagen se registran como campos identificados de este registro. Las imágenes de impresiones palmares enviadas a otros organismos serán tratadas por ellos para extraer la información que necesiten con fines de identificación.

Los datos de la imagen se obtendrán directamente de la persona por medio de un escáner o a partir de una ficha de una impresión palmar con otros soportes en los que se encuentre la impresión.

Cualquiera de los métodos que se utilicen para captar la imagen de la huella palmar debe proporcionar un juego completo de imágenes de cada mano. El juego comprenderá el canto de la mano en posición cubital como una imagen separada y la zona entera de la palma desde la muñeca hasta la punta de los dedos en una o dos imágenes. Si se emplean dos imágenes para la palma completa, la imagen inferior irá desde la muñeca hasta la parte superior de la zona interdigital (la tercera falange) y comprenderá las regiones tenar e hipotenar. La imagen superior abarcará desde la base de la zona interdigital hasta la punta de los dedos. Esto permite una superposición suficiente entre las dos imágenes en la zona interdigital de la palma. Al encajar la estructura de las crestas y otros detalles de esta zona en las dos imágenes, el experto puede garantizar que las dos imágenes proceden de la misma palma.

Dado que una transacción de impresión palmar puede tener finalidades diversas, es posible que incluya una o varias zonas de imagen específicas de la palma o la mano. El registro palmar completo de una persona incluirá normalmente el canto en posición cubital y la imagen o las imágenes de la palma completa de cada mano. Dado que el registro de imagen de campo identificado solo puede tener un campo binario, se necesitará un registro de tipo-15 para cada canto en posición cubital y uno o dos para cada palma completa. Por tanto, la representación normal de las impresiones palmares de un individuo en una transacción normal requerirá de cuatro a seis registros del tipo-15.

8.1. *Campos del registro de tipo-15*

Los párrafos siguientes describen los datos de cada uno de los campos de un registro de tipo-15.

En un registro de tipo-15 los datos están ordenados en campos numerados. Los dos primeros campos siguen un orden preestablecido y la imagen estará en el último campo del registro. En el cuadro 8 figura cada uno de los campos del registro de tipo-15 con su correspondiente código de condición, según sea obligatorio «M», en inglés, o facultativo «O», en inglés, el número de campo, el nombre, el tipo de carácter empleado, el tamaño del campo y las veces que puede aparecer. Basándose en un número de campo de tres dígitos, en la última columna aparece señalado el número máximo de bytes que puede contener. Si se emplean más dígitos para el número de campo, el número máximo de bytes aumentará. Las cifras que figuran como mínimo y máximo de tamaño de campo incluyen todos los caracteres de separación empleados en el campo. El cálculo máximo de bytes comprende el número de campo, la información y todos los caracteres de separación, incluido el final, «GS».

8.1.1. Campo 15.001: Longitud del registro lógico (Logical record length) (LEN)

Este campo ASCII obligatorio recoge el cómputo total de bytes del registro de tipo-15. El campo 15.001 indicará la longitud del registro contando todos los caracteres de cada uno de sus campos, incluidos los separadores.

8.1.2. Campo 15.002: Carácter de designación de la imagen (Image designation character) (IDC)

Este campo ASCII obligatorio se empleará para identificar la imagen de la impresión palmar incluida en el registro. Este IDC deberá coincidir con el IDC que figure en el campo de contenido del fichero (CNT) del registro de tipo-1.

8.1.3. Campo 15.003: Tipo de impresión (Impression type) (IMP)

Este campo ASCII obligatorio de un byte indicará cómo se tomó la impresión palmar. Deberá figurar el código apropiado de los que figuran en el cuadro 9.

8.1.4. Campo 15.004: Organismo de origen/ORI (Source agency/ORI) (SRC)

Este campo ASCII obligatorio identificará a la administración u organización que tomó la impresión palmar que contiene el registro. En general, en este campo figurará el ORI del organismo que tomó la imagen. Se compone de dos elementos de información con el siguiente formato: CP/organismo.

El primer elemento de información contiene el código de país de Interpol y tiene una longitud de dos caracteres alfanuméricos. El segundo, organismo, es un campo de texto libre de un máximo de 32 caracteres alfanuméricos, que identifica al organismo.

8.1.5. Campo 15.005: Fecha de la impresión palmar (Palmprint capture date) (PCD)

Este campo ASCII obligatorio recogerá la fecha en que se tomó la imagen de la impresión palmar. La fecha se expresará en el formato de ocho dígitos siguiente: CCYYMMDD. En donde CCYY representa el año en que se tomó la imagen, MM el mes en decenas y unidades, DD las decenas y unidades correspondientes al día del mes. Así, por ejemplo, 20000229 hace referencia al 29 de febrero de 2000. La fecha completa debe ser una fecha real.

8.1.6. Campo 15.006: Longitud de línea horizontal (Horizontal line length) (HLL)

Este campo ASCII obligatorio indica el número de píxeles que contiene cada línea horizontal de la imagen transmitida.

8.1.7. Campo 15.007: Longitud de línea vertical (Vertical line length) (VLL)

Este campo ASCII obligatorio indica el número de líneas horizontales que contiene la imagen transmitida.

8.1.8. Campo 15.008: Unidades de medida (Scale units) (SLC)

Este campo ASCII obligatorio indicará las unidades empleadas para describir la densidad de píxeles de la imagen. Se empleará el «1» si se trata de píxeles por pulgada y el «2» si se trata de píxeles por centímetros. Si aparece un «0» no se proporciona la escala. En este caso la proporción de píxeles se obtendrá dividiendo la HPS por la VPS.

8.1.9. Campo 15.009: Escala horizontal de píxel (Horizontal pixel scale) (HPS)

Este campo ASCII obligatorio indica en números enteros la densidad de píxeles de las líneas horizontales siempre y cuando en el campo SLC se haya expresado la unidad de medida con un «1» o un «2», en caso contrario indica el número de píxeles del componente horizontal.

8.1.10. Campo 15.010: Escala vertical de píxel (Vertical pixel scale) (VPS)

Este campo ASCII obligatorio indica en números enteros la densidad de píxeles de las líneas verticales siempre y cuando en el campo SLC se haya expresado la unidad de medida con un «1» o un «2», en caso contrario indica el número de píxeles del componente vertical.

Cuadro 8: Presentación del registro de tipo-15 de imagen de impresión palmar de resolución variable

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15 001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15 002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15 003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15 004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15 005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15 006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15 007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15 008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15 009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15 010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15 011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15 012	bits PER PIXEL	N	2	3	1	1	10
PLP	M	15 013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15 014 15 019	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
COM	O	15 020	COMMENT	AN	2	128	0	1	128
RSV		15 021 15 199	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
UDF	O	15 200 15 998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	15 999	IMAGE DATA	B	2	—	1	1	—

Cuadro 9: Tipo de impresión 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 compresión (Compression algorithm) (CGA)

Este campo ASCII obligatorio especificará el algoritmo utilizado para comprimir imágenes en escala de grises. Una entrada NONE en este campo indica que los datos que contiene este registro no están comprimidos. Para aquellas imágenes que vayan a comprimirse, este campo incluirá el método elegido para la compresión de las imágenes de las impresiones dactilares de las fichas decadactilares. Los códigos de compresión válidos se definen en el apéndice 7.

8.1.12. Campo 15.012: Bits por píxel (Bits per pixel) (BPX)

Este campo ASCII obligatorio contendrá el número de bits utilizados para representar un píxel. Este campo contendrá una entrada de «8» para los valores normales de la escala de grises del «0» al «255». Cualquier entrada en este campo que sea superior o inferior a «8» representará un píxel de escala de grises con precisión aumentada o disminuida, respectivamente.

Cuadro 10: Códigos, áreas y tamaños 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
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: Posición de la impresión palmar (Palmprint position) (PLP)

Este campo etiquetado obligatorio contendrá la posición de la impresión palmar que encaja con la imagen de la impresión palmar. El número de código decimal que corresponda a la posición conocida o más probable de la impresión palmar se tomará del cuadro 10 y se introducirá como subcampo ASCII de dos caracteres. El cuadro 10 enumera también las áreas y dimensiones máximas de la imagen de cada una de las posiciones posibles de la impresión palmar.

8.1.14. Campo 15.014-019: Reservados para definición futura (Reserved for future definition) (RSV)

Estos campos quedan reservados para incluirlos en revisiones futuras de esta norma. Ninguno de estos campos va a usarse en el presente nivel de revisión. Si se presenta alguno de estos campos, no se tendrá en cuenta.

8.1.15. Campo 15.020: Observación (Comment) (COM)

Este campo optativo puede usarse para incluir observaciones u otros datos en texto ASCII con los datos de la imagen de la impresión palmar.

8.1.16. Campos 15.021-199: Reservados para definición futura (Reserved for future definition) (RSV)

Estos campos quedan reservados para incluirlos en revisiones futuras de esta norma. Ninguno de estos campos va a usarse en el presente nivel de revisión. Si se presenta alguno de estos campos, no se tendrá en cuenta.

8.1.17. Campos 15.200-998: Campos definidos por el usuario (User-defined fields) (UDF)

Estos campos podrán ser definidos por el usuario y se utilizarán para exigencias futuras. Su tamaño y su contenido serán definidos por el usuario y serán conformes con el organismo receptor. Si existen, contendrán información textual en ASCII.

8.1.18. Campo 15.999: Datos de imagen (Image data) (DAT)

Este campo contendrá todos los datos procedentes de una imagen tomada de una impresión palmar. Llevará asignado siempre el número de campo 999 y deberá ser el último campo físico del registro. Por ejemplo: «15.999:» irá seguido de los datos de la imagen en representación binaria. Cada píxel de datos en escala de grises sin comprimir se cifrará en principio en ocho bits (256 niveles de gris) contenidos en un solo byte. Si la entrada del campo BPX 15.012 es mayor o menor que 8, el número de bytes necesarios para abarcar un píxel será distinto. Si se recurre a la compresión, los datos del píxel se comprimirán según la técnica de compresión especificada en el campo CGA.

8.2. *Final del registro de imagen de impresión palmar de resolución variable de tipo-15*

Por motivos de coherencia, inmediatamente a continuación del último byte de datos del campo 15.999, se colocará un separador «FS» para separarlo del siguiente registro. Dicho separador deberá incluirse en el campo de longitud del registro de tipo-15.

8.3. *Otros registros de imagen de impresión palmar de resolución variable de tipo-15*

En el archivo podrán incluirse más registros de tipo-15. Para cada imagen de impresión palmar añadida, es necesario un registro lógico de tipo-15 completo junto con el separador «FS».

Cuadro 11: Números máximos de candidatos aceptados para la verificación por transmisión

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 búsqueda:

TP/TP: ficha decadactilar contra ficha decadactilar

LT/TP: impresión dactilar latente contra ficha decadactilar

LP/PP: impresión palmar latente contra impresión palmar

TP/UL: ficha decadactilar contra impresión dactilar latente no resuelta

LT/UL: impresión dactilar latente contra impresión dactilar latente no resuelta

PP/ULP: impresión palmar contra impresión palmar latente no resuelta

LP/ULP: impresión palmar latente contra impresión palmar latente no resuelta

9. ***Apéndices al capítulo 2 (intercambio de datos dactiloscópicos)***

9.1. *Apéndice 1 Códigos separadores 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]) Esta es la posición definida en la norma ASCII.

9.2. *Apéndice 2 Cálculo del carácter alfanumérico de control*

Para TCN y TCR (campos 1.09 y 1.10):

El número correspondiente al carácter de control se genera aplicando la fórmula siguiente:

(YY * 10^8 + SSSSSSSS) Modulo 23

siendo YY y SSSSSSSS, respectivamente, los valores numéricos de las dos últimas cifras del año y el número de serie.

El carácter de control se genera a continuación a partir del cuadro de búsqueda que figura más abajo.

Para CRO (campo 2.010)

El número correspondiente al carácter de control se genera aplicando la fórmula siguiente:

(YY * 10^6 + NNNNNN) Modulo 23

siendo YY y NNNNNN, respectivamente, los valores numéricos de las dos últimas cifras del año y el número de serie.

El carácter de control se genera a continuación a partir del cuadro de búsqueda que figura más abajo.

Cuadro de búsqueda de los caracteres de control

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. *Apéndice 3 Códigos de caracteres*

Código ANSI de 7 bits para intercambio de información

ASCII Character Set

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

9.4. *Apéndice 4 Resumen de las transacciones*

Registro de tipo-1 (obligatorio)

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

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

En la columna «Condition»:

O = optativo; M = obligatorio; C = condicionado si la transacción es respuesta al organismo de origen

Registro de tipo-2 (obligatorio)

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

En la columna «Condition»:

O = optativo; M = obligatorio; C = condicionado si se dispone de datos

* = si la transmisión de los datos es conforme con el Derecho nacional (no contemplado en la Decisión 2008/615/JAI)

9.5. *Apéndice 5 Definiciones de los registros de tipo-1*

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	1003:1{US}15{RS}2{US}00{RS}4 {US}01{RS}4{US}02{RS}4{US}03 {RS}4{US}04{RS}4{US}05{RS}4 {US}06{RS}4{US}07{RS}4{US}08 {RS}4{US}09{RS}4{US}10{RS}4 {US}11{RS}4{US}12{RS}4{US}13 {RS}4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1 004:CPS{GS}
DAT	M	1.005	Date	N	1 005:20050101{GS}
PRY	M	1.006	Priority	N	1 006:4{GS}
DAI	M	1.007	Destination Agency	1*	1 007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1 008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1 009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1 010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1 011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1 012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1 013: INT-I{US}4.22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1 014:20050101125959Z

En la columna «Condition»: O = optativo; M = obligatorio; C = condicionado

En la columna «Character type»: A = alfabético; N = numérico; B = binario

1* los caracteres permitidos para el nombre del organismo son [«0..9», «A..Z», «a..z», «_», «.», «», «—»]

9.6. *Apéndice 6 Definiciones de los registros de tipo-2*

Cuadro A.6.1: Transacción CPS- y 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}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
INF	O	2.063	Additional Information	1*	2 063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2 320:1{GS}

Cuadro A.6.2: Transacción 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}
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}

Cuadro A.6.3: Transacción 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}

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
ERM	M	2.074	Status/Error Message Field	AN	2 074: 201: IDC - 1 FIELD 1 009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2 003 INVALID SYSTEM INFORMATION {GS}

Cuadro A.6.4: Transacción MPS- y 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}

En la columna «Condition»: O = optativo; M = obligatorio; C = condicionado

En la columna «Character type»: A = alfabético; N = numérico; B = binario

1* los caracteres permitidos son [«0..9», «A..Z», «a..z», «_», «.», «», «—», «,»]

9.7. *Apéndice 7 Códigos de compresión de la escala de grises*

Códigos de compresión

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

9.8. *Apéndice 8 Especificación de correo*

Para mejorar el volumen de trabajo interno el destinatario de una transacción PRUEM debe rellenarse con el código de país (CP) del Estado miembro que envía el mensaje y el tipo de transacción (campo TOT 1.004).

Formato: CP/tipo de transacción

Ejemplo: «DE/CPS»

El cuerpo del correo puede quedar en blanco.

CAPÍTULO 3**: Intercambio de datos de matriculación de vehículos**

1. ***Enumeración común de datos para la búsqueda automatizada de datos de matriculación de vehículos***

1.1. *Definiciones*

Las definiciones de elementos de datos obligatorios y elementos de datos optativos fijados en el artículo 16.4 son las siguientes:

Obligatorios (M):

El dato debe ser comunicado cuando la información esté disponible en el registro nacional de un Estado miembro. Por consiguiente, existe la obligación de intercambiar la información cuando esté disponible.

Optativos (O):

El dato puede ser comunicado cuando la información esté disponible en el registro nacional de un Estado miembro. Por consiguiente, no existe obligación de intercambiar la información aun cuando esté disponible.

Se añade una indicación (Y) a cada elemento del conjunto de datos que se distingue como importante en relación con la Decisión 2008/615/JAI.

1.2. *Búsqueda de vehículos, propietarios y titulares*

1.2.1. Activadores de la búsqueda

Hay dos modos diferentes de buscar la información definida en el siguiente párrafo:

— por número de bastidor (VIN) y fecha y hora de referencia (optativo),

— por número de licencia, número de bastidor (VIN) (optativo), y fecha y hora de referencia (optativo).

Mediante estos criterios, se producirá la información relativa a uno y, a veces, varios vehículos. Si debe producirse la información de un solo vehículo, todos los elementos se producen en una sola respuesta. Si se halla más de un vehículo, el Estado miembro requerido mismo podrá determinar qué elementos serán producidos, si todos los elementos o solo los necesarios para restringir la búsqueda (por ejemplo, por razones de intimidad o por razones de resultados).

Los elementos necesarios para restringir la búsqueda se ilustran en el apartado 1.1.2.1. En el apartado 1.2.2.2 se describe el conjunto completo de informaciones.

Cuando la búsqueda se haga por número de bastidor y fecha y hora de referencia, la búsqueda podrá hacerse en uno de los Estados participantes o en todos.

Cuando la búsqueda se haga por número de licencia y fecha y hora de referencia, la búsqueda deberá hacerse en un Estado miembro en particular.

En principio, la fecha y hora reales se utilizan para hacer una búsqueda, pero esta puede hacerse con una fecha y hora de referencia del pasado. Cuando se haga una búsqueda con fecha y hora de referencia del pasado y no exista información histórica en el registro del Estado miembro en particular por no estar registrada dicha información, la información real podrá producirse indicando que la información es información real.

1.2.2. Conjunto de datos

1.2.2.1. Elementos producidos que son necesarios para ajustar la búsqueda

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

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

(1) M = obligatorio cuando esté disponible en el registro nacional, O = optativo.
(2) Todos los atributos asignados específicamente por el Estado miembro se indican con Y.
(3) Abreviatura documental armonizada, véase la Directiva 1999/37/CE del Consejo, de 29 de abril de 1999.

1.2.2.2. Conjunto completo de datos

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

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

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

(1) M = obligatorio cuando esté disponible en el registro nacional; O = optativo.
(2) Abreviatura documental armonizada, véase la Directiva 1999/37/CE del Consejo, de 29 de abril de 1999.
(3) En Luxemburgo se usan dos documentos de registro de vehículos independientes.

2. ***Seguridad de los datos***

2.1. *Generalidades*

El programa informático Eucaris maneja la información protegida con destino a los demás Estados miembros y se comunica a los sistemas heredados secundarios de los Estados miembros por medio de XML. Los Estados miembros intercambian mensajes enviándolos directamente al destinatario. El centro de datos de un Estado miembro está conectado a la red TESTA de la UE.

Los mensajes XML enviados por la red están cifrados. La técnica de cifrado de estos mensajes es SSL. Los mensajes enviados al sistema secundario serán mensajes XML de texto en claro, pues la conexión entre el programa y el sistema secundario se producirá en un entorno protegido.

Se proveerá un programa cliente que podrá usar cada Estado miembro para buscar en su propio registro o en el de otros Estados miembros. Los clientes serán identificados mediante identificación de usuario y contraseña o certificado de cliente. La conexión a un usuario podrá estar cifrada, pero esto es responsabilidad de cada Estado miembro.

2.2. *Características de seguridad relacionadas con el intercambio de mensajes*

El diseño de seguridad se basa en una combinación de firma HTTPS y firma XML. Dentro de esta alternativa, se recurre a la firma XML para firmar todos los mensajes enviados al servidor, pudiéndose autenticar al emisor del mensaje mediante una comprobación de la firma. La SSL de una sola cara (únicamente un certificado de servidor) se utiliza para proteger la confidencialidad e integridad del mensaje en tránsito y brinda protección contra los ataques de supresión/reproducción e inserción. En lugar de desarrollar programas informáticos a la medida para aplicar la SSL de dos caras, se ejecuta la firma XML. El uso de esta firma es más cercano al mapa de servicios web que la SSL de dos caras y, por tanto, resulta más estratégico.

Aunque la firma XML puede ejecutarse de varias maneras, el enfoque elegido es utilizar dicha firma como parte de la WWS (Web Services Security), la cual especifica la manera de utilizar la firma XML. Dado que la WSS se basa en la norma SOAP, es lógico adherir a dicha norma en la mayor medida posible.

2.3. *Características de seguridad no relacionadas con el intercambio de mensajes*

2.3.1. Autenticación de los usuarios

Los usuarios de la aplicación web Eucaris se autentican a sí mismos utilizando un nombre de usuario y una palabra clave. Dado que se utiliza la autenticación estándar de Windows, los Estados miembros podrán mejorar el nivel de autenticación de los usuarios, si fuera necesario, mediante la utilización de certificados de cliente.

2.3.2. Cometidos de los usuarios

La aplicación web Eucaris acepta diferentes cometidos de usuarios. Cada grupo de servicios tiene su propia autorización. Así, por ejemplo, los usuarios (exclusivos) de las «funciones del Tratado Eucaris» no pueden utilizar las «funciones del Tratado de Prüm». Los servicios del administrador están separados de los cometidos habituales de los usuarios finales.

2.3.3. Registro y rastreo del intercambio de datos

El registro de todos los tipos de mensajes es facilitado por la aplicación informática Eucaris. Una función de administrador permite al administrador nacional determinar qué mensajes se registran: solicitudes de usuarios finales, solicitudes recibidas de otros Estados miembros, información facilitada a partir de registros nacionales, etc.

La aplicación puede configurarse para utilizar una base de datos interna para dicho registro o una base de datos externa (Oracle). La decisión sobre qué mensajes deben registrarse depende evidentemente de los dispositivos de registro en cualquiera de los sistemas legados y de las aplicaciones de cliente que estén conectadas.

El encabezamiento de cada mensaje contiene información sobre el Estado miembro solicitante, la organización solicitante dentro de dicho Estado miembro y el usuario implicado. También se indica el motivo de la solicitud.

Mediante el registro combinado en el Estado solicitante y el Estado que responde, es posible realizar un rastreo completo de cualquier intercambio de mensajes (por ejemplo, a solicitud de un ciudadano implicado).

El registro es configurado por el cliente web de Eucaris (menú «Administración» [Administration], configuración «Registro» [Logging]). La función de registro la ejecuta el sistema central [Core System]. Una vez autorizado el registro, el mensaje completo (encabezamiento y cuerpo) es almacenado en un archivo de registro. El nivel de registro puede fijarse para cada servicio recibido y para cada tipo de mensaje que pase por el sistema central.

Niveles de registro

Son posibles los siguientes niveles de registro:

Privado [Private] — El mensaje está registrado: el registro NO está disponible para el servicio de extracción del registro, pero está disponible (únicamente a nivel nacional) para las auditorías y la resolución de problemas.

Ninguno [None] — El mensaje no está registrado bajo ningún concepto.

Tipos de mensajes

El intercambio de información entre Estados miembros consta de varios mensajes, de los que se ofrece una representación esquemática en el gráfico que figura más adelante:

Los posibles tipos de mensajes (en el gráfico mostrado para el sistema central de Eucaris del Estado miembro X) son los siguientes:

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

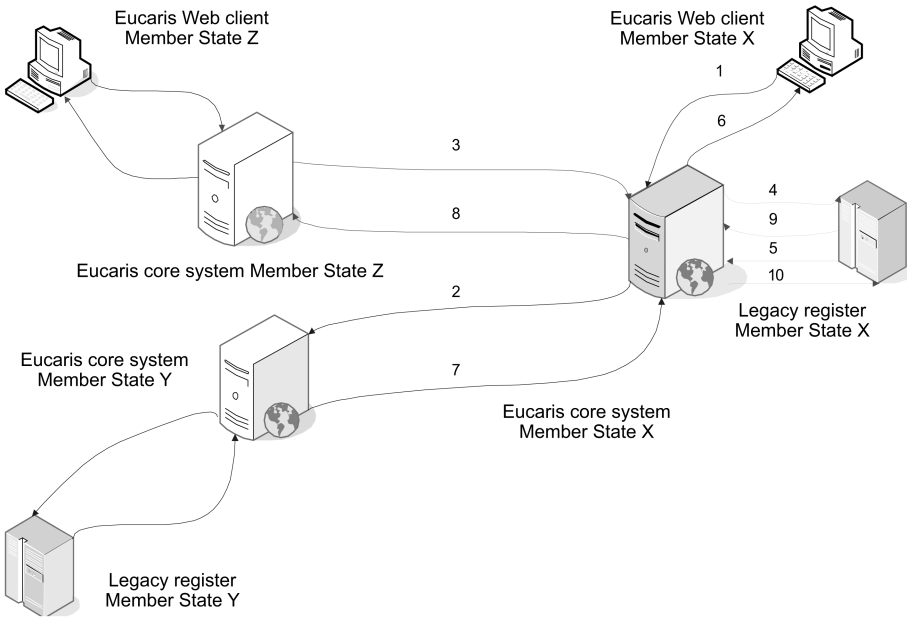
En el gráfico se muestran los siguientes intercambios de información:

— Información solicitada desde el Estado miembro X al Estado miembro Y — flechas azules. A esta solicitud y a la respuesta corresponden los tipos de mensajes 1, 2, 7 y 6, respectivamente.

— Información solicitada desde el Estado miembro Z al Estado miembro X — flechas rojas. A esta solicitud y a la respuesta corresponden los tipos de mensajes 3, 4, 9 y 8, respectivamente.

— Información solicitada desde el registro legado a su sistema central (esta ruta incluye también una solicitud procedente de un cliente a la medida tras el registro legado) — flechas verdes. A este tipo de solicitud corresponden los tipos de mensajes 5 y 10.

Gráfico: Tipos de mensajes para el registro



2.3.4. Módulo de seguridad hardware

No se utiliza ningún módulo de seguridad *hardware*.

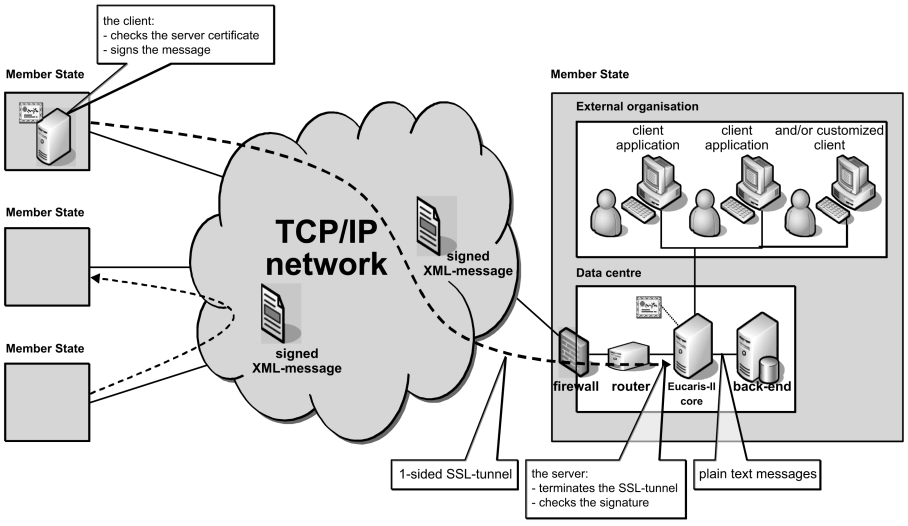
Un módulo de seguridad *hardware* (HSM) ofrece una buena protección de la clave utilizada para firmar mensajes de firma e identificar los servidores. Aunque ello aumenta el nivel general de seguridad, adquirir o mantener un HSM resulta caro y no existen requisitos para decidirse por un HSM FIPS 140-2 de nivel 2 o 3. Dado que se utiliza una red cerrada que reduce las amenazas de modo efectivo, se ha decidido no utilizar inicialmente un HSM. En caso necesario podría añadirse a la arquitectura un HSM, por ejemplo para obtener una acreditación.

3. *Condiciones técnicas del intercambio de datos*

3.1. *Descripción general de la aplicación Eucaris*

3.1.1. Visión de conjunto

La aplicación Eucaris conecta a todos los Estados miembros participantes en una red de malla en la que cada Estado miembro comunica directamente con otro Estado miembro. No se requiere ningún componente central para la comunicación que deba establecerse. La aplicación Eucaris se ocupa de la comunicación segura a los demás Estados miembros y facilita la comunicación a los sistemas legados en fase final de los Estados miembros que recurran a XML. En el gráfico siguiente se ilustra dicha arquitectura:



Los Estados miembros intercambian mensajes enviándolos directamente al destinatario. El centro de datos de un Estado miembro está conectado a la red utilizada para el intercambio de mensajes (TESTA). Para acceder a la red TESTA, los Estados miembros se conectan a dicha red a través de su portal nacional. Para conectarse a la red debe utilizarse un cortafuegos *(firewall)*. Asimismo, un encaminador *(router)* debe conectar la aplicación Eucaris al cortafuegos. Según la opción elegida para proteger los mensajes, un certificado es utilizado por el encaminador o por la aplicación Eucaris.

Se facilita una aplicación de cliente, la cual puede utilizarse en un Estado miembro para consultar su propio registro o los registros de otros Estados miembros. La aplicación de cliente se conecta con Eucaris. Los clientes son identificados bien mediante una identificación de usuario y una contraseña, bien mediante un certificado de cliente. La conexión con un usuario de una organización exterior (por ejemplo, la policía) puede cifrarse, pero esto es responsabilidad de cada Estado miembro en particular.

3.1.2. Ámbito de aplicación del sistema

El ámbito de aplicación de Eucaris se limita a las operaciones implicadas en el intercambio de información entre las autoridades responsables de la matriculación en los diferentes Estados miembros y a una presentación básica de dicha información. Los procedimientos y tratamientos automáticos en que debe utilizarse la información quedan fuera del ámbito de aplicación del sistema.

Los Estados miembros pueden elegir entre utilizar las funciones de cliente Eucaris o establecer su propia aplicación de cliente habitual. En el cuadro que figura a continuación se indica qué aspectos del sistema de Eucaris son de uso obligatorio o están recomendados y qué aspectos son de uso facultativo o pueden ser determinados libremente por los Estados miembros.

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

[1] M = uso o cumplimiento obligatorio; O = uso o cumplimiento optativo.

3.2. *Requisitos funcionales y no funcionales*

3.2.1. Funciones genéricas

En esta sección se describen de modo general las principales funciones genéricas.

N°	Descripción
1.	El sistema permite a las autoridades responsables de la matriculación en los diferentes Estados miembros intercambiar mensajes de solicitud y respuesta de manera interactiva.
2.	El sistema incluye una aplicación de cliente que permite a los usuarios finales enviar sus solicitudes y presentar la información de respuesta para el tratamiento manual.
3.	El sistema facilita una «transmisión» *(broadcasting)* que permite a un Estado miembro enviar una solicitud a todos los demás Estados miembros. Las respuestas recibidas son fusionadas por la aplicación central en una respuesta de mensaje a la aplicación de cliente (esta función se denomina «Multiple Country Inquiry»).
4.	El sistema es capaz de tratar diferentes tipos de mensajes. Los cometidos de los usuarios, la autorización, el encaminamiento *(routing)*, la firma y el registro son definidos para cada servicio específico.
5.	El sistema permite a los Estados miembros intercambiar lotes de mensajes o mensajes que contengan un número elevado de solicitudes o respuestas. Estos mensajes son tratados de manera asíncrona.
6.	Si el Estado miembro receptor está temporalmente indisponible, el sistema pone en una lista de espera los mensajes asíncronos y garantiza su envío una vez que el receptor vuelva a estar disponible.
7.	El sistema almacena los mensajes asíncronos hasta que puedan ser procesados.
8.	El sistema solo proporciona acceso a las aplicaciones Eucaris de otros Estados miembros, no a las diversas organizaciones de los mismos. Es decir, cada autoridad responsable de la matriculación actúa como pasarela única entre sus usuarios finales nacionales y las autoridades correspondientes de los demás Estados miembros.
9.	Es posible definir a usuarios de diferentes Estados miembros en un servidor Eucaris y autorizarles de conformidad con los derechos del Estado miembro de que se trate.
10.	En los mensajes se incluye información relativa al Estado miembro solicitante, a la organización y al usuario final.
11.	El sistema facilita el registro del intercambio de mensajes entre los diferentes Estados miembros, por una parte, y la aplicación central y los sistemas de matriculación nacionales, por otra parte.
12.	El sistema permite a un secretario específico, que es una organización o un Estado miembro designados de manera explícita para esta tarea, recoger la información registrada sobre los mensajes enviados o recibidos por todos los Estados miembros participantes, con vistas a elaborar informes estadísticos.
13.	Cada Estado miembro indicará qué información registrada se ha puesto a la disposición del secretario y qué información es «privada».
14.	El sistema permite a los administradores nacionales de cada Estado miembro obtener estadísticas de utilización.
15.	El sistema permite incluir a nuevos Estados miembros mediante operaciones administrativas simples.

3.2.2. Utilización

N°	Descripción
16.	El sistema proporciona una interfaz para el tratamiento de mensajes mediante sistemas en fase final o legados y permite la integración de la interfaz del usuario en dichos sistemas (interfaz a la medida del usuario).
17.	El sistema es de fácil aprendizaje, se explica por sí mismo y contiene texto de ayuda.
18.	El sistema está documentado para asistir a los Estados miembros en la integración, las actividades operativas y el mantenimiento en el futuro (por ejemplo, guías de referencia, documentación funcional y técnica, guía operativa, etc.).
19.	La interfaz del usuario es multilingüe y brinda varias posibilidades al usuario final para seleccionar una lengua preferente.
20.	La interfaz del usuario brinda varias posibilidades al administrador local para traducir a la lengua nacional la información que figura en pantalla y la información codificada.

3.2.3. Fiabilidad

N°	Descripción
21.	El sistema está concebido como un sistema operativo sólido y fiable que es tolerante con los errores de los operadores y se reactivará sin problemas en caso de corte de electricidad u otros contratiempos. Se podrá reactivar el sistema sin pérdida de datos, o solo de manera mínima.
22.	El sistema debe dar resultados estables y reproducibles.
23.	El sistema está concebido para funcionar de manera fiable. Se puede ejecutar con una configuración que garantice una disponibilidad del 98 % (mediante redundancia, la utilización de servidores que hagan copias de seguridad, etc.) en cada comunicación bilateral.
24.	Se puede utilizar parte del sistema, incluso en caso de fallo de algunos de sus componentes (si el Estado miembro C está desconectado, los Estados miembros A y B pueden seguir comunicándose entre sí.
25.	El tiempo de reactivación tras un fallo grave debería ser inferior a un día. El tiempo de desconexión debería poderse reducir al mínimo recurriendo a la asistencia a distancia, por ejemplo a través de un servicio central.

3.2.4. Prestaciones

N°	Descripción
26.	El sistema puede utilizarse 24 horas al día los siete días de la semana. Este marco temporal también se exige a los sistemas legados de los Estados miembros.
27.	El sistema responde rápidamente a las demandas del usuario independientemente de cualquier otra tarea de fondo. Ello se exige también a los sistemas legados de las Partes, a fin de garantizar un tiempo de respuesta aceptable. Se considera aceptable un tiempo total de respuesta de diez segundos como máximo.
28.	El sistema está concebido como un sistema para varios usuarios, de manera que las tareas de fondo puedan proseguir mientras el usuario realiza tareas en un primer plano.
29.	El sistema está concebido de manera que sea adaptable para poder asumir un posible aumento del número de mensajes cuando se añadan nuevas funciones, nuevas organizaciones o nuevos Estados miembros.

3.2.5. Seguridad

N°	Descripción
30.	El sistema es adecuado (por ejemplo, en sus medidas de seguridad) para el intercambio de mensajes que contengan datos personales sensibles relativos a la vida privada (por ejemplo, propietarios o poseedores de automóviles) clasificados como restringidos UE).
31.	El sistema es mantenido de tal manera que se impide el acceso a los datos por parte de personas no autorizadas.
32.	El sistema incluye un servicio para la gestión de los derechos y autorizaciones de los usuarios finales nacionales.
33.	Los Estados miembros pueden comprobar la identidad del emisor (a nivel del Estado miembro) mediante la firma XML.
34.	Los Estados miembros deben autorizar de modo explícito a otros Estados miembros a solicitar información específica.
35.	El sistema ofrece, a nivel de la aplicación, una política de plena seguridad y cifrado compatible con el nivel de seguridad exigido en tales situaciones. La exclusividad e integridad de la información quedan garantizadas por la utilización de la firma XML y del cifrado mediante tunelización *(tunelling)* SSL.
36.	Todo intercambio de mensajes puede ser rastreado mediante el registro.
37.	Se brinda protección contra los ataques de borrado (un tercero suprime un mensaje) y los ataques de repetición o inserción (un tercero repite o inserta un mensaje).
38.	El sistema utiliza certificados de un tercero de confianza (TC).
39.	El sistema es capaz de tratar diferentes certificados para cada Estado miembro, den función del tipo de mensaje o servicio.

N°	Descripción
40.	Las medidas de seguridad a nivel de la aplicación son suficientes para permitir la utilización de redes no acreditadas.
41.	El sistema es capaz de utilizar nuevas técnicas de seguridad, como por ejemplo un cortafuegos XML.

3.2.6. Adaptabilidad

N°	Descripción
42.	El sistema puede ampliarse con nuevos mensajes y nuevas funciones. Debido al desarrollo centralizado de los componentes de la aplicación, los costes de adaptación son mínimos.
43.	Los Estados miembros pueden definir nuevos tipos de mensajes para una utilización bilateral. No se exige a todos los Estados miembros que presten asistencia a todos los tipos de mensaje.

3.2.7. Asistencia y mantenimiento

N°	Descripción
44.	El sistema brinda posibilidades para un servicio central u operadores en relación con la red y los servidores en los diferentes Estados miembros.
45.	El sistema brinda posibilidades para la asistencia a distancia a través de un servicio central.
46.	El sistema brinda posibilidades para el análisis de problemas.
47.	El sistema puede extenderse a nuevos Estados miembros.
48.	La aplicación puede ser instalada fácilmente por personas que tengan una formación en tecnología de la información (TI) y experiencia en dicho sector.
49.	El sistema permite la realización permanente de pruebas y un entorno de aceptación.
50.	Los costes anuales de mantenimiento y asistencia se han reducido al mínimo, observándose las normas del mercado y concibiéndose la aplicación de manera tal que se requiera la menor asistencia posible por parte de un servicio central.

3.2.8. Requisitos de diseño

N°	Descripción
51.	El sistema está diseñado y documentado para que pueda funcionar durante muchos años.
52.	El sistema se ha diseñado de tal forma que sea independiente del suministrador de red.
53.	El sistema se adapta a los soportes físicos y lógicos existentes en los Estados miembros mediante una interacción con los sistemas de registro que utilicen la tecnología estándar abierta de servicios web (XML, XSD, SOAP, WSDL, HTTP(s), servicios web, WSS, X.509, etc.).

3.2.9. Normas aplicables

N°	Descripción
54.	El sistema se adapta a los puntos relativos a la protección de datos expuestos en el Reglamento (CE) n° 45/2001 (artículos 21, 22 y 23) y en la Directiva 95/46/CE.
55.	El sistema cumple la normativa IDA.
56.	El sistema es compatible con UTF8.

CAPÍTULO 4**: Evaluación**

1. ***Procedimiento de evaluación con arreglo al artículo 20 (formulación de decisiones de conformidad con el artículo 25, apartado 2, de la Decisión 2008/615/JAI)***

1.1. *Cuestionario*

El Grupo pertinente del Consejo elaborará un cuestionario relativo a cada uno de los intercambios automatizados de datos que se indican en el capítulo 2 de la Decisión 2008/615/JAI.

Tan pronto como un Estado miembro considere que cumple los requisitos previos para compartir datos en la categoría que corresponda, deberá responder al cuestionario pertinente.

1.2. *Ensayo piloto*

Con vistas a evaluar los resultados del cuestionario, el Estado miembro que desee comenzar a compartir datos llevará a cabo un ensayo piloto junto con uno o más Estados miembros que ya compartan datos con arreglo a la Decisión del Consejo. El ensayo piloto se realizará poco antes o después de la visita de evaluación.

Las condiciones y modalidades del ensayo piloto las determinará el Grupo pertinente del Consejo y se basarán en un acuerdo individual previo con el Estado miembro de que se trate. Los Estados miembros que participen en el ensayo piloto decidirán los pormenores prácticos.

1.3. *Visita de evaluación*

Con vistas a evaluar los resultados del cuestionario, se llevará a cabo una visita de evaluación en el Estado miembro que desee comenzar a compartir datos.

Las condiciones y modalidades de esta visita las determinará el Grupo pertinente del Consejo y se basarán en un acuerdo individual previo entre el Estado miembro de que se trate y el equipo de evaluación. El Estado miembro de que se trate permitirá al equipo de evaluación comprobar el intercambio automatizado de datos en la categoría o categorías que deban evaluarse, para lo cual, en particular, organizará un programa para la visita, el cual tendrá en cuenta las solicitudes formuladas por el equipo de evaluación.

En el plazo de un mes, el quipo de evaluación elaborará un informe sobre la visita de evaluación y lo remitirá al Estado miembro de que se trate para que este formule observaciones. Si procede, el informe será objeto de una revisión por el equipo de evaluación, que se basará en las observaciones de ese Estado miembro.

El equipo de evaluación estará compuesto por un máximo de tres expertos designados por los Estados miembros que participen en el intercambio automatizado de datos en las categorías que deban evaluarse y que tengan experiencia en la categoría de datos de que se trate, posean la adecuada habilitación de seguridad de rango nacional para tratar estas cuestiones y estén dispuestos a participar al menos en una visita de evaluación en otro Estado miembro. Se invitará a la Comisión a unirse al equipo de evaluación en calidad de observadora.

Los miembros del equipo de evaluación respetarán el carácter confidencial de la información que obtengan en el desempeño de su cometido.

1.4. *Informe al Consejo*

Para que el Consejo adopte una decisión con arreglo al artículo 25, apartado 2, de la Decisión 2008/615/JAI, se le presentará un informe de evaluación general en el que se resuman los resultados de los cuestionarios.

2. ***Procedimiento de evaluación con arreglo al artículo 21***

2.1. *Estadísticas e informe*

Cada Estado miembro recopilará estadísticas sobre los resultados del intercambio automatizado de datos. Para garantizar la posibilidad de su comparación, el modelo para dichas estadísticas lo compondrá el Grupo pertinente del Consejo.

Las estadísticas se presentarán cada año a la Secretaría General, la cual hará un breve balance del año transcurrido, así como a la Comisión.

Además, una vez al año como máximo, se solicitará a los Estados miembros que faciliten información adicional sobre la ejecución administrativa, técnica y financiera del intercambio automatizado de datos, en la medida en que dicha información sea necesaria para analizar y mejorar el proceso. Se presentará un informe al Consejo en el que se tenga en cuenta dicha información.

2.2. *Revisión*

Dentro de un plazo razonable, el Consejo examinará el mecanismo de evaluación aquí descrito y, si fuera necesario, lo revisará.

3. Reuniones de expertos

En el Grupo pertinente del Consejo, se reunirán expertos para organizar y ejecutar los procedimientos de evaluación antes mencionados, así como para compartir experiencias y debatir posibles mejoras. Si procede, los resultados de estos debates de expertos se incluirán en el informe a que se refiere el punto 2.1.