OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Part 10: Estructura lógica de datos (LSD) para el almacenamiento de datos biométricos y de otro tipo en el circuito integrado (CI) sin contacto

Arpobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Part 10: Estructura lógica de datos (LSD) para el almacenamiento de datos biométricos y de otro tipo en el circuito integrado (CI) sin contacto

Arpobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

Publicado por separado en español, árabe, chino, francés, inglés y ruso
por la ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL
999 Robert-Bourassa Boulevard, Montreal, Quebec, Canadá H3C 5H7

En el sitio web http://www.icao.int/Security/FAL/TRIP pueden obtenerse descargas
e información adicional

Doc 9303, *Documentos de viaje de lectura mecánica*
Parte 10 — *Estructura lógica de datos (LDS) para el almacenamiento de datos biométricos y de otro tipo en el circuito integrado (CI) sin contacto*
Pedido núm.: 9303P10
ISBN 978-92-9265-559-4 (versión impresa)

ENMIENDAS

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de productos y servicios*; el Catálogo y sus suplementos pueden consultarse en el sitio web de la OACI: www.icao.int. Las casillas en blanco facilitan la anotación de estas enmiendas.

REGISTRO DE ENMIENDAS Y CORRIGENDAS

ENMIENDAS		
Núm.	Fecha	Anotada por

CORRIGENDAS		
Núm.	Fecha	Anotado por

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la OACI, juicio alguno sobre la condición jurídica de ninguno de los países, territorios, ciudades o áreas, o de sus autoridades, ni respecto a la delimitación de sus fronteras o límites.

ÍNDICE

Página

Página

1. ALCANCE

En la Parte 10 del Doc 9303 se define la estructura lógica de datos (LDS) para eMRTD necesaria para la interoperabilidad mundial. Se definen también las especificaciones para la organización de los datos en el circuito integrado (CI) sin contacto. Esto exige la identificación de todos los elementos de datos obligatorios y opcionales y un ordenamiento o agrupamiento establecido de los elementos de datos que DEBE seguirse para lograr la interoperabilidad mundial de la lectura electrónica del pasaporte electrónico (eMRTD).

En la Parte 10 del Doc 9303 se proporcionan especificaciones para permitir que Estados e integradores implanten un CI sin contacto en un documento de viaje electrónico. En esta parte se definen todos los elementos de datos obligatorios y opcionales, estructuras de ficheros y perfiles de aplicaciones para el CI sin contacto.

La octava edición del Doc 9303 incorpora las especificaciones para los registros de viaje opcionales, los registros de visados y las aplicaciones biométricas adicionales (conocidas como aplicaciones de la LDS2) como extensión de la aplicación del eMRTD obligatoria (conocida como LDS1).

La Parte 10 deberá leerse conjuntamente con:

- Parte 1 — *Introducción*;
- Parte 3 — *Especificaciones comunes a todos los MRTD*;
- Parte 4 — *Especificaciones para los pasaportes de lectura mecánica (MRP) y otros MRTD de tamaño DV3*;
- Parte 5 — *Especificaciones para documentos oficiales de viaje de lectura mecánica (MROTD) de tamaño DV1*;
- Parte 6 — *Especificaciones para documentos oficiales de viaje de lectura mecánica (MROTD) de tamaño DV2*;

y las partes pertinentes sobre CI sin contacto en:

- Parte 9 — Empleo de identificación biométrica y almacenamiento electrónico de datos en los MRTD;
- Parte 11 — *Mecanismos de seguridad para los MRTD*;
- Parte 12 — *Infraestructura de clave pública para los MRTD*.

2. ESTRUCTURA DEL DOC 9303-10

La Parte 10 del Doc 9303 está organizada por secciones con el fin de incluir:

Especificaciones comunes a las aplicaciones de la LDS1 y LDS2:

- Atributos comunes;
- Todas las órdenes para LDS1 y LDS2; y
- Ficheros elementales comunes (EF) para LDS1 y LDS2;

Especificaciones para la aplicación de la LDS1 del eMRTD;

Especificaciones para la aplicación de la LDS2:

- Registros de viaje;
- Registros de visados;
- datos biométricos adicionales; y
- especificaciones para las condiciones de acceso al fichero LDS2.

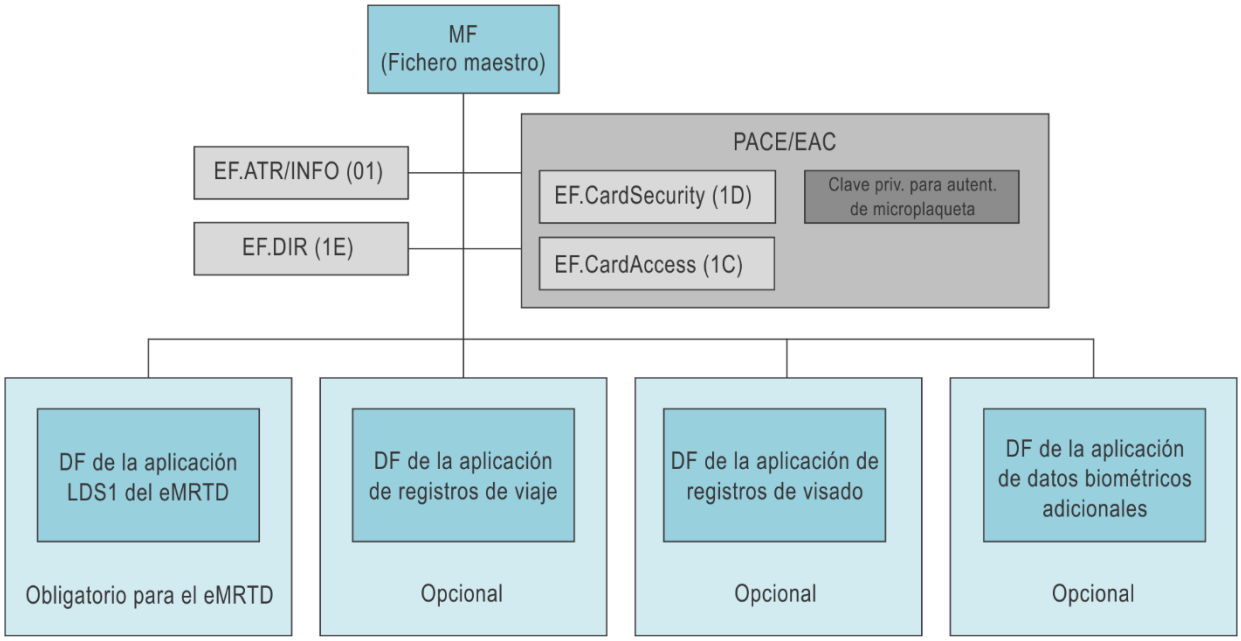


Figura 1. Aplicaciones para LDS1 y LDS2

El eMRTD puede admitir una, varias o todas las aplicaciones siguientes:

- aplicación del eMRTD LDS1, OBLIGATORIA;
- aplicación de los registros de viaje LDS2, OPCIONAL;
- aplicación de los registros de visados LDS2, OPCIONAL;
- aplicación de los datos biométricos adicionales LDS2, OPCIONAL.

3. ESPECIFICACIONES COMUNES A LDS1 Y LDS2

3.1 Requisitos mínimos de interoperabilidad

Los siguientes SERÁN los requisitos mínimos de interoperabilidad de los pasaportes electrónicos de proximidad de CI sin contacto:

- ajustarse a [ISO/IEC 14443-1], [ISO/IEC 14443-2], [ISO/IEC 14443-3], [ISO/IEC 14443-4] incluyendo todas las enmiendas y corrigendas conexas;
- ajustarse a la especificación de ensayos de [ISO/IEC 10373-6] incluyendo todas las enmiendas y corrigendas conexas;
- interfaz de señales Tipo A o Tipo B;
- apoyo para estructura de fichero definida en [ISO/IEC 7816-4] para ficheros transparentes de longitud variable;
- apoyo para una o más aplicaciones y órdenes apropiadas definidas en [ISO/IEC 7816-4], según se especifica en el Doc 9303;

3.2 Características eléctricas

La potencia de radiofrecuencia y la interfaz de señal SERÁN las definidas en [ISO/IEC14443-2]. Se aconseja un mínimo de velocidad de transmisión de 424 kilobits por segundo. El uso de los elementos EMD especificados en [ISO/IEC 14443-2] es OPCIONAL.

3.3 Características físicas

Se recomienda que el tamaño del área de antena de acoplamiento se ajuste a la [ISO/IEC 14443-1] Clase 1 (tamaño de antena ID-1) solamente.

3.4 Protocolo de transmisión

El eMRTD APOYARÁ un protocolo de transmisión en semidúplex definido en [ISO/IEC14443-4]. El eMRTD ADMITIRÁ los protocolos de transmisión de Tipo A o B y la inicialización y protocolos de anticolisión y transmisión con arreglo a ISO/IEC 14443.

3.4.1 Petición de orden y respuesta a petición

El CI sin contacto RESPONDERÁ a una petición de orden de Tipo A (REQA) o petición de orden de Tipo B (REQB) con respuesta a petición de Tipo A (ATQA) o respuesta a petición de Tipo B (ATQB), según corresponda.

3.4.2 Identificador aleatorio e identificador fijo para el CI sin contacto

El eMRTD puede servir como “radiofaro” en el cual el CI sin contacto emite un identificador único (UID) para el Tipo A, y un PUPI para el Tipo B cuando se le activa inicialmente. Esto puede permitir la identificación de la autoridad emisora. La [ISO/IEC 14443] permite elegir la opción de si el eMRTD presenta un identificador fijo, asignado unívocamente para solo eMRTD, o un número aleatorio, que es diferente en cada comienzo del diálogo de comunicación. Algunos Estados

expedidores prefieren implantar un número único por razones de seguridad o cualquier otro motivo. Otros expedidores dan mayor preferencia a preocupaciones sobre el carácter privado de los datos y la posibilidad de rastrear personas debido al uso de identificadores CI fijos.

La elección de una u otra opción no disminuye el interfuncionamiento dado que un terminal lector que cumpla con ISO/IEC 14443 entenderá ambos métodos. SE RECOMIENDA el uso de identificadores de CI aleatorios pero los Estados PUEDEN optar por aplicar UID únicos para el Tipo A o PUPI únicos para el Tipo B.

3.5 Conjunto de comandos

Todos los comandos, formatos y sus bytes de estado se definen en [ISO/IEC 7816-4] y en [ISO/IEC 7816-8] con la excepción del comando FILE AND MEMORY MANAGEMENT. El conjunto de comandos mínimo que ha de ser admitido por la LDS1 del eMRTD DEBE ser el siguiente:

SELECT (SELECCIONAR);
READ BINARY (LEER BINARIO).

Se reconoce que será necesario contar con órdenes adicionales para establacer el entorno de seguridad correcto y aplicar las disposiciones de seguridad opcionales que se identifican en el Doc 9303-11. La implantación de los mecanismos especificados en el Doc 9303-11 requiere el apoyo de las siguientes órdenes adicionales:

GET CHALLENGE (OBTENER PUESTA A PRUEBA);
EXTERNAL AUTHENTICATE/ MUTUAL AUTHENTICATE (AUTENTICACIÓN EXTERNA/ AUTENTICACIÓN MUTUA);
INTERNAL AUTHENTICATE (AUTENTICACIÓN INTERNA);
MANAGE SECURITY ENVIRONMENT (GESTIONAR ENTORNO DE SEGURIDAD);
GENERAL AUTHENTICATE (AUTENTICACIÓN GENERAL).

Si están presentes aplicaciones de la LDS2 opcionales, el eMRTD ADMITIRÁ adicionalmente las siguientes órdenes:

Para la aplicación de los registros de viaje:
READ RECORD (LEER REGISTRO);
APPEND RECORD (ADJUNTAR REGISTRO);
SEARCH RECORD (BUSCAR EN REGISTRO);
FILE AND MEMORY MANAGEMENT (GESTIÓN DE FICHEROS Y MEMORIA);
PERFORM SECURITY OPERATION (PSO) (REALIZAR OPERACIONES DE SEGURIDAD).

Para la aplicación de los registros de visados:
READ RECORD (LEER REGISTRO);
APPEND RECORD (AÑADIR REGISTRO);
SEARCH RECORD (BUSCAR EN REGISTRO);
FILE AND MEMORY MANAGEMENT (GESTIÓN DE FICHEROS Y MEMORIA);
PERFORM SECURITY OPERATION (PSO) (REALIZAR OPERACIONES DE SEGURIDAD).

Para la aplicación de los datos biométricos adicionales:
UPDATE BINARY (ACTUALIZAR BINARIO);
READ RECORD (LEER REGISTRO);
APPEND RECORD (ADJUNTAR REGISTRO);
SEARCH RECORD (BUSCAR EN REGISTRO);
ACTIVATE (ACTIVAR);
FILE AND MEMORY MANAGEMENT (GESTIÓN DE FICHEROS Y MEMORIA);
PERFORM SECURITY OPERATION (PSO) (REALIZAR OPERACIONES DE SEGURIDAD).

En el Doc 9303-11 figuran más detalles sobre los protocolos de comandos.

3.5.1 SELECT

La LDS1 del eMRTD admite dos métodos de selección de estructura, concretamente el identificador de fichero y el identificador EF breve. Los lectores admiten por lo menos uno de ambos métodos. El identificador de fichero y el identificador EF breve son OBLIGATORIOS para el sistema operacional del CI sin contacto, pero son opcionales para el lector.

3.5.2 READ BINARY

El apoyo al comando READ BINARY con un byte INS impar por un eMRTD es CONDICIONAL. El eMRTD APOYARÁ esta variedad de comando si apoya los grupos de datos con 32 768 bytes o más.

3.6 Formatos de comandos y opciones de parámetros (LDS1 y LDS2)

3.6.1 Selección del DF de la aplicación por medio del comando SELECT

Las aplicaciones tienen que seleccionarse por su nombre DF que indica el identificador de la aplicación (AID). Después de la selección de una aplicación puede accederse al fichero que está dentro de dicha aplicación.

Nota.— Los nombres DF tienen que ser únicos. Por consiguiente, la selección de una aplicación utilizando el nombre del DF puede efectuarse desde donde se requiera.

3.6.1.1 Selección de fichero maestro

Tabla 1. Comando SELECT para la selección del MF

CLA	‘00’
INS	‘A4’
P1	‘00’
P2	‘0C’
Campo Lc	Ausente
Campo de datos	Ausente
Campo Le	Ausente

Respuesta para el comando SELECT

Campo de datos	Ausente
SW1-SW2	Procesamiento normal ‘9000’ Otros valores para indicar errores de comprobación o ejecución

Nota.— Se RECOMIENDA no utilizer el comando SELECT MF.

3.6.1.2 Selección del DF de la aplicación

Se seleccionará un DF de la aplicación utilizando el comando SELECT con el nombre DF que indica el identificador de la aplicación (AID). A continuación se muestran los parámetros para el comando de la unidad de datos de protocolo de aplicación (APDU):

Tabla 2. Comando SELECT con AID para la selección del DF de la aplicación

CLA	'00'
INS	'A4'
P1	'04'
P2	'0C'
Campo Lc	Longitud del campo de datos del comando
Campo de datos	Nombre del DF (AID)
Campo Le	Ausente

Respuesta para el comando SELECT

Campo de datos	Ausente
SW1-SW2	Procesamiento normal '9000' Otros valores para indicar errores de comprobación o ejecución

3.6.2 Selección del EF mediante el comando SELECT

El EF se selecciona por medio del comando SELECT con identificador EF. Cuando se selecciona el EF, es preciso asegurarse de que se ha seleccionado previamente el DF de la aplicación que almacena el EF.

Tabla 3. Comando SELECT con identificador de fichero para la selección de EF

CLA	'00' / '0C'
INS	'A4'
P1	'02'
P2	'0C'
Campo de Lc	'02'
Campo de datos	Identificador de fichero
Campo de Le	Ausente

Respuesta para el comando SELECT

Campo de datos	Ausente
SW1-SW2	Procesamiento normal '9000' Otros valores para indicar errores de verificación o ejecución

El eMRTD APOYARÁ el comando SELECT con el identificador de fichero según se especifica en la Tabla 3. El sistema de inspección APOYARÁ por lo menos uno de los métodos siguientes:

- el comando SELECT con identificador de fichero según se especifica en la Tabla 3;
- el comando READ BINARY con código INS par y un identificador EF breve según se especifica en la tabla 5.

3.6.3 Lectura de datos del EF (READ BINARY)

Existen dos métodos principales para leer los datos del eMRTD: seleccionar el EF y luego leer los datos del EF seleccionado o leer los datos directamente utilizando el identificador EF breve (SFI). Para el eMRTD es OBLIGATORIO admitir el identificador EF breve; por ello, se RECOMIENDA que el sistema de inspección utilice el identificador EF breve.

3.6.3.1 Lectura de datos de un EF seleccionado (fichero transparente)

Tabla 4. Comando READ BINARY para un EF seleccionado

CLA	'00' / '0C'
INS	'B0'
P1	
P2	
Campo Lc	Ausente
Campo de datos	Ausente
Campo Le	Presente para codificar Ne > 0

Respuesta para el comando READ BINARY

Campo de datos	Lectura de datos
SW1-SW2	Procesamiento normal '9000' Otros valores para indicar errores de comprobación o ejecución

3.6.3.2 Lectura de datos mediante el identificador EF (fichero transparente)

Tabla 5. Comando READ BINARY con identificador EF breve

CLA	'00' / '0C'
INS	'B0'
P1	Identificador EF breve
P2	Desplazado
Campo Lc	Ausente
Campo de datos	Ausente
Campo Le	Presente para codificar Ne > 0. Número máximo de bytes previsto del campo de datos de la respuesta

Respuesta para el comando READ BINARY

Campo de datos	Lectura de datos
SW1-SW2	Procesamiento normal '9000' Otros valores para indicar errores de comprobación o ejecución

3.6.4 Apoyo Lc/Le ampliado

Dependiendo del tamaño de los objetos criptográficos (p. ej., claves públicas, firmas), las APDU con campos de longitud ampliada DEBEN utilizarse para enviar estos datos a la microplaqueta del eMRTD. Los detalles sobre los campos de longitud ampliada figuran en la [ISO/IEC 7816-4].

3.6.4.1 Longitud ampliada y microplaquetas de eMRTD

Para las microplaquetas de eMRTD, el apoyo del campo de longitud ampliada es CONDICIONAL. Si los algoritmos criptográficos y los tamaños de claves seleccionados por el Estado expedidor exigen el uso del campo de longitud ampliada, las microplaquetas del eMRTD ADMITIRÁN el campo de longitud ampliada. Si la microplaqueta del eMRTD admite el campo de longitud ampliada, DEBE indicarse en ATS o en EF.ATR/INFO, según se especifica en [ISO/IEC 7816-4].

3.6.4.2 Terminales

Para los terminales la admisión del campo de longitud ampliada es OBLIGATORIA. Un terminal DEBERÍA examinar si la admisión del campo de longitud ampliada se indica en el ATR/ATS de la microplaqueta del eMRTD o en EF.ATR/INFO antes de utilizar esta opción. El terminal NO DEBE utilizar el campo de longitud ampliada para las APDU con comandos distintos de los siguientes a menos que el tamaño exacto de la memoria intermedia de entrada y de salida de la microplaqueta del eMRTD esté explícitamente declarado en ATS o en EF.ATR/INFO.

- MSE: Set KAT;
- GENERAL AUTHENTICATE.

3.6.5 Encadenamiento de comandos

El encadenamiento de comandos DEBE utilizarse para que el comando GENERAL AUTHENTICATE enlace la secuencia de comandos con la ejecución del protocolo. El encadenamiento de comandos NO DEBE utilizarse para otros fines a menos que se indique claramente en la microplaqueta. En la [ISO/IEC 7816-4] figuran detalles sobre encadenamiento de comandos.

3.6.6 EF mayor de 32 767 bytes

El tamaño máximo de un EF es normalmente 32 767 bytes, pero algunos CI apoyan ficheros mayores. Se requiere un formato de comando y una opción de parámetro READ BINARY diferentes para tener acceso a la suma de datos cuando el desplazamiento es mayor de 32 767. Este formato de comando DEBERÍA utilizarse después de haberse determinado la longitud de la plantilla y la necesidad de acceder a los datos en la zona de datos ampliada. Por ejemplo, si la zona de datos contiene objetos de datos biométricos múltiples, puede no ser necesario leer toda la zona de datos. Una vez que el desplazamiento de la zona de datos sea mayor que 32 767, SE EMPLEARÁ este formato de comando. El desplazamiento se coloca en el campo de comandos en vez de en los parámetros P1 y P2.

Tabla 6. Formato de comando READ BINARY cuando el desplazamiento para EF es superior a 32 767 bytes

CLA	'00' / '0C'
INS	'B1'
P1	Véase la tabla 7
P2	
Campo Lc	Longitud del campo de datos del comando
Campo de datos	DO'54' desplazamiento
Campo Le	Presente para la codificación Ne > 0. Número máximo de bytes esperados en el campo de datos de la respuesta

Respuesta para el comando READ BINARY

Campo de datos	DO'53' discrecional
SW1-SW2	Procesamiento normal '9000' Otros valores para indicar errores de comprobación o ejecución

Tabla 7. Codificación en P1-P2 del comando READ BINARY con INS = B1

P1								P2								
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b8**	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Significado**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	EF seleccionado
0	0	0	0	0	0	0	0	0	0	0	No son todos iguales					Identificador EF breve
No son todos cero								X	X	X	X	X	Identificador EF			

Este campo de longitud y el campo de valor en el objeto de datos BER-TLV son de longitud variable y pueden codificarse de diferentes maneras (véase [ISO/IEC 7816-4]: “campos de longitud BER-TLV”).

Por razones de actuación, la comunicación entre el eMRTD y el terminal DEBERÍA mantenerse lo más breve posible. Por consiguiente, los campos de longitud y de valor en el objeto de datos BER-TLV DEBERÍAN ser lo más breves posibles. Esto se aplica no solamente a los objetos de datos desplazados en las órdenes READ BINARY de INS impar sino también a todos los otros objetos de datos BER-TLV intercambiados entre el eMRTD y el terminal.

Ejemplos de desplazamiento codificado de campo de datos:

- Desplazamiento: ‘0001’ se codifica como rótulo = ‘54’ Longitud = ‘01’ valor = ‘01’;
- Desplazamiento: ‘FFFF’ se codifica como rótulo= ‘54’ Longitud = ‘02’ valor = ‘FFFF’.

Los siguientes comandos READ BINARY ESPECIFICARÁN el desplazamiento en el campo de datos. El comando READ BINARY final DEBERÍA pedir la zona de datos restante.

Con respecto a [ISO/IEC 7816-4], en el valor de desplazamiento no se especifican limitaciones cuando el bit 1 de INS is pone a 1 para permitir un uso más amplio.

Nota 1.— En algunos casos, hay eMRTD en los que los comandos B1 y el tradicional B0 READ Binary no podrían superponerse. En otras palabras, el B0 solo debería utilizarse para leer los primeros 32 767 bytes y el B1 los bytes de 32 K en adelante. Para otros fines podría haber una pequeña superposición de 256 bytes alrededor del umbral 32 767 para permitir una transición más fluida entre B0 y B1. Para este último grupo, B1 podría utilizarse a partir del mismo comienzo del fichero, es decir, con un desplazamiento a partir de 0 para permitir el uso de la misma orden a efectos de leer todo el contenido.

Nota 2.— El sistema de inspección no ha de utilizar el byte INS impar si el tamaño de una EF es de 32 767 bytes o menos.

3.7 Comandos y gestión de registros (LDS2)

Los registros de viaje, los registros de visados y los certificados DEBEN almacenarse en el EF, en las respectivas aplicaciones, y tener una estructura lineal con registros de tamaño variable. Véanse las figuras 4 y 5.

Los registros dentro de cada EF DEBEN llevar como referencia un número de registro. Cada número de registro DEBE ser único y secuencial (el cero para referenciar el registro seleccionado queda fuera del alcance de este documento).

Dentro de cada EF que admite una estructura lineal, los números de registro DEBEN asignarse secuencialmente cuando se añaden por ejemplo según el orden de creación; el primer registro (número uno) es el registro que se creó primero.

DEBEN usarse los siguientes comandos [ISO/IEC 7816-4] para el acceso a los registros:

- APPEND RECORD Adición de registros de viaje, visados, certificados;
- READ RECORD(S) Lectura de uno o más registros de viaje, visados, certificados;
- SEARCH RECORD Búsqueda de uno o más registros de viaje, visados, certificados.

Nota.— Los acrónimos utilizados en esta subsección se definen en [ISO/IEC 7816-4].

3.7.1 Comando APPEND RECORD

El comando inicia la adición de un registro nuevo al final de una estructura lineal.

Tabla 8. Comando APPEND RECORD

CLA	'0C'
INS	'E2'
P1	'00' (ningún otro valor es válido)
P2	Véase la tabla 10
Campo Lc	Longitud del campo de datos del comando
Campo de datos	Registro que debe añadirse
Campo Le	Ausente

Tabla 9. Respuesta APPEND RECORD

Campo de datos	Ausente
SW1-SW2	Procesamiento normal '9000'; '6A84' El fichero no dispone de suficiente espacio de memoria; '6700' Longitud incorrecta (el registro que debe añadirse supera la longitud máxima especificada); Otros valores para indicar errores de comprobación o ejecución

Tabla 10. Codificación de P2 en el comando APPEND RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Significado
x	x	x	x	x	-	-	-	Identificador EF breve
-	-	-	-	-	0	0	0	Cualquier otro valor es RFU

3.7.2 Comando READ RECORD

El comando devuelve el contenido completo o parcial de uno o más registros direccionados del ED seleccionado. Dependiendo del tamaño del registro y del contenido del campo Le, el campo de datos de la respuesta contiene uno de los elementos siguientes:

- la primera parte del registro direccionado;
- uno (o más) registros completos direccionados;
- uno (o más) registros completos direccionados seguidos de la primera parte del registro siguiente.

En [ISO/IEC 7816-4] figuran detalles y en el apéndice H figura un ejemplo de lectura de un registro de viaje.

En la figura 2 se ilustra el campo de datos de la respuesta. La comparación de N_r con la estructura TLV indica si el registro único (lectura de un registro) o el último registro (lectura de todos los registros) está incompleto, completo o rellenado.

Tabla 11. Comando READ RECORD

CLA	‘0C’	
INS	‘B2’	
P1	Número de registro (‘00’ se refiere al registro actual)	
P2	Véase la tabla 13	
Campo Lc	Ausente	
Campo de datos	INS = ‘B2’	Ausente
Campo Le	Número máximo de bytes que se han de leer codificados como campo de longitud ampliada; Le = ‘00 00 00’ (cualquier otro valor queda fuera del alcance de la especificación)	

Tabla 12. Respuesta READ RECORD

Campo de datos	Datos leídos
SW1-SW2	Procesamiento normal ‘9000’; ‘6A83’ (Registro no encontrado); Otros valores para indicar errores de comprobación o ejecución.

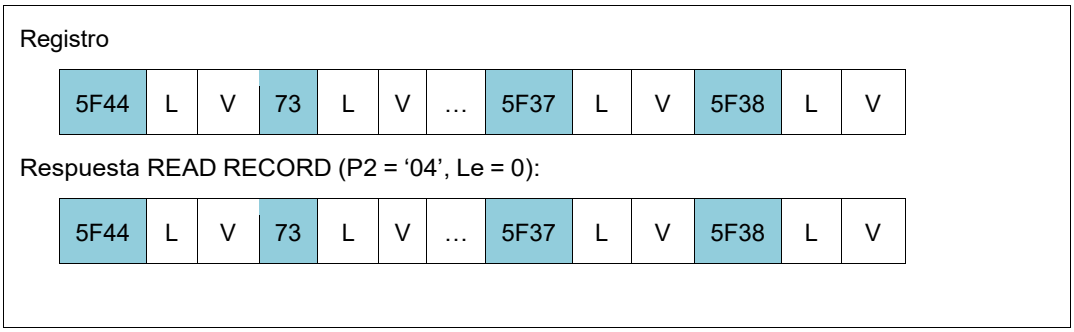
Tabla 13. Codificación de P2 con el comando READ RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Significado
x	x	x	x	x	-	-	-	Identificador EF breve
-	-	-	-	-	1	x	x	**Número de registro indicado en P1**
-	-	-	-	-	1	0	0	— Lectura del registro P1
-	-	-	-	-	1	0	1	— Lectura de todos los registros, desde el P1 hasta el último

Nota 1.— Otras combinaciones de bits quedan fuera del alcance de esta especificación. Si el campo Le solo contiene bytes puestos a ‘00’, entonces el comando debería leer completamente el registro individual solicitado o la secuencia de registros solicitada, dependiendo de los bits 3, 2 y 1 de P2 y dentro del límite de la longitud máxima admitida para el campo Le ampliado.

Nota 2.— El comando READ RECORD con campos de longitud corta queda fuera del alcance de esta especificación.

Caso a — Completar la lectura de un registro (el campo Le solo contiene bytes puestos a ‘00’)



Caso b — Leer varios registros hasta el final del fichero (el campo Le solo contiene bytes puestos a ‘00’)

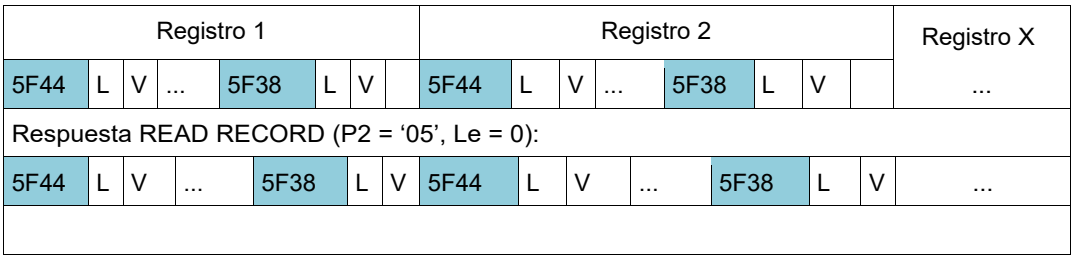


Figura 2. Campos de datos de la respuesta

3.7.3 Comando SEARCH RECORD

El comando inicia una búsqueda en los registros almacenados dentro del EF respectivo. El campo de datos del comando contiene el DO’7F76’ de gestión de registros, que define la referencia del fichero, la configuración de búsqueda y la cadena de búsqueda (véase la tabla 17). El campo de datos de la respuesta devuelve el DO’7F76’ de gestión de registros, que contiene uno o más DO’02’ y el número de registro que corresponde a los criterios de búsqueda dentro del EF direccionado.

En un EF que admite registros de tamaño variable con una estructura lineal, PUEDE que la búsqueda NO tenga en cuenta los registros con una ventana de búsqueda más corta que la cadena de búsqueda.

Tabla 14. Comando SEARCH RECORD

CLA	‘0C’
INS	‘A2’
P1	‘00’
P2	Véase la tabla 16
Campo Lc	Longitud del campo de datos del comando
Campo de datos	DO’7F76’ de gestión de registros (véase la tabla 17)
Campo Le	‘00’ (longitud corta) o ‘00 00’ (longitud ampliada)

Tabla 15. Respuesta SEARCH RECORD

Campo de datos	DO'7F76' de la plantilla de gestión de registros que contiene un DO'51' de referencia de fichero con uno o más números enteros DO'02' y con un número de registro que se corresponde con los criterios de búsqueda
SW1-SW2	Procesamiento normal '9000'; Aviso '6282': Búsqueda fallida Otros valores para indicar errores de comprobación o ejecución

Nota.— El campo de datos de la respuesta puede estar ausente si no se encuentra correspondencia.

Tabla 16. Codificación de P2 para el comando SEARCH RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Significado
1	1	1	1	1	0	0	0	Búsqueda en el registro a través de múltiples EF
Cualquier otro valor es RFU.								

Tabla 17. Plantilla de gestión de registros para una búsqueda mejorada en múltiples registros

Rótulo	Valor				Notas
'7F76'					DO de gestión de registros
	Rótulo	**Valor**			
	'51'	Identificador de archivo o identificador EF breve			DO de referencia de fichero
	'A1'				Plantilla de configuración de búsqueda
		Rótulo	**Valor**		
		'80'	'00' / '30'		Parámetro de configuración de búsqueda - búsqueda por orden ascendente de número de registro - en todas las etapas búsqueda al nivel de los bytes - terminación de la búsqueda: '00' – búsqueda en todos los registros direccionados '30' – terminación de la búsqueda después de la primera correspondencia
		'B0'			Plantilla de la ventana de búsqueda
			Rótulo	**Valor**	
			'02'	Desplazamiento	
			'02'	Número de bytes	

	Rótulo	**Valor**			
	‘A3’				Plantilla de la cadena de búsqueda
		Rótulo	**Valor**		
		‘B1’			
			Rótulo	**Valor**	
			‘81’	Cadena de búsqueda	

Nota 1.— No se admite un DO desplazado vacío en la plantilla de la ventana de búsqueda.

Nota 2.— Si la plantilla de la ventana de búsqueda utiliza el valor ‘00’ para el número de bytes, la LDS2 de la microplaqueta del eMRTD DEBE buscar todos los bytes del desplazamiento en los registros.

Nota 3.— El comando SEARCH RECORD admite solo los DO especificados en la tabla 17. Esto implica que el comando SEARCH RECORD admite exactamente un DO referencia de fichero en el DO de la gestión de registros y exactamente una cadena de búsqueda en la plantilla de la cadena de búsqueda. El comando PUEDE no tener en cuenta DO adicionales o contestar con un código de error si se usan DO adicionales.

3.8 Gestión de ficheros transparentes y otros (LDS2)

Los EF transparentes de datos biométricos adicionales los crea quien expide la LDS2 del eMRTD en el estado desactivado operacional (el mecanismo de creación queda fuera del alcance de esta especificación). En el estado desactivado, puede seleccionarse, escribirse, actualizarse y leerse el EF con las autorizaciones apropiadas.

Los siguientes comandos [ISO/IEC 7816-4] DEBEN usarse para escribir y leer los EF transparentes con datos biométricos adicionales:

- UPDATE BINARY Escritura de los datos biométricos adicionales;
- READ BINARY Lectura de los datos biométricos adicionales.

El siguiente comando [ISO/IEC 7816-9] DEBE usarse para activar el EF transparente después de cumplir debidamente las condiciones de acceso de lectura y escritura de la LSD2:

- ACTIVATE Activación del EF de datos biométricos adicionales.

Nota.— Los acrónimos utilizados en esta subsección se definen en [ISO/IEC 7816-4].

En el estado activado, puede seleccionarse y leerse el EF con las autorizaciones apropiadas (relacionadas con el estado activado) y ninguna autorización de ningún tipo permite la escritura o adición del EF transparente.

El comando FILE AND MEMORY MANAGEMENT (FMM) DEBE usarse antes de la escritura para determinar si hay suficiente espacio de memoria disponible en el EF.

El IS DEBE usar la siguiente secuencia de escritura para el EF.Biometrics:

- El primer comando UPDATE BINARY (INS impar) DEBE contener los siguientes DO en el campo de datos:

  - El DO'54', que contiene el '00' desplazado;

  - El DO'53', que PUEDE contener el primer bloque de los datos que han de almacenarse. Este DO PUEDE estar vacío ('53 00'); y

  - El DO'C0' propio, que indica el tamaño total del EF (tamaño de memoria para asignar), es opcional.

Nota 1.— La LDS2 del eMRTD PUEDE usar información del tamaño del EF en DO'C0' para la asignación de la memoria interna (p. ej., para la asignación de memoria dinámica explícita). Si la LDS2 del eMRTD no admite el DO de información del tamaño del EF (p. ej., el expedidor ha asignado la memoria estáticamente, o la LDS2 del eMRTD admite una reasignación de memoria dinámica implícita del EF), entonces la LDS2 del eMRTD PUEDE no tener en cuenta el DO'C0', proceder con la lectura del primer bloque del EF y devolver '9000', o PUEDE devolver el error '6A80' en el caso de un parámetro incorrecto en el campo de datos del comando.

Nota 2.— Si la LDS2 del eMRTD devuelve un error en respuesta a UPDATE BINARY con el DO'C0' propio, entonces el IS DEBE enviar el comando estándar UPDATE BINARY (INS impar) conforme a [ISO/IEC 7816-4], con DO'54' y DO'53' de desplazamiento cero, sin el DO'C0'.

- Los comandos UPDATE BINARY (INS impar, sin DO'C0') subsiguientes DEBERÍAN usar el desplazamiento n+1, donde n indica el número de bytes escritos hasta el momento en EF.Biometrics, i. e. el terminal DEBERÍA escribir secuencialmente los datos del EF sin que falte ni se superponga nada entre los dos comandos UPDATE BINARY consecutivos.

- El comando READ BINARY PUEDE usarse después de cualquier comando UPDATE BINARY para verificar los datos escritos en el EF.

- El comando ACTIVATE DEBE finalizar la personalización de EF.Biometrics desactivando permanentemente la escritura en el EF.

3.8.1 Comando UPDATE BINARY

Un CI sin contacto que admite la aplicación de los datos biométricos adicionales DEBE admitir el comando UPDATE BINARY con el byte INS impar 'D7' de acuerdo con la tabla 18.

El valor del objeto de datos de desplazamiento BER-TLV del campo de datos del comando especifica el desplazamiento; el valor del objeto de datos discrecional BER-TLV del campo de datos del comando especifica cuáles son los datos que han de escribirse; el valor del objeto de datos del tamaño del fichero BER-TLV opcional del campo de datos del comando especifica el tamaño total del EF. Los campos de longitud de estos objetos de datos BER-TLV deberían codificarse de la forma más corta posible.

Cuando el campo de datos del comando UPDATE BINARY tiene un DO'C0' propio, el bit 8 del byte CLA del comando APDU DEBE ponerse en 1 (CLA = '8C').

Tabla 18. Comando UPDATE BINARY con INS impar

CLA	‘0C’ / ‘8C’
INS	‘D7’
P1	Identificador de fichero ‘00 00’ identifica el EF actual
P2	
Lc	Longitud del campo de datos del comando
Campo de datos	Objeto de datos de desplazamiento (rótulo ‘54’) || Objeto de datos discrecional (rótulo ‘53’) || Objeto de datos del tamaño del fichero (rótulo ‘C0’) (opcional)
Le	Ausente

Tabla 19. Respuesta UPDATE BINARY

Campo de datos	Ausente
SW1-SW2	Procesamiento normal ‘9000’; ‘6A84’ (No hay suficiente espacio de memoria en el fichero) ‘6A80’: Parámetros incorrectos en el campo de datos del comando (p. ej., no se admite el DO’C0) ‘6982’: Estado de seguridad no satisfecho: El EF.Biometrics está en estado activado Otros valores para indicar errores de comprobación o ejecución

Si el IS no sigue la secuencia UPDATE BINARY especificada en la sección 3.8 (i. e. el primer UPDATE BINARY no empieza en el desplazamiento 0), la LDS2 de la microplaqueta del eMRTD PUEDE terminar el comando UPDATE BINARY con un error.

3.8.2 Comando ACTIVATE

El comando ACTIVATE inicia la transición del EF de datos biométricos adicionales seleccionado del estado desactivado al estado activado.

Tabla 20. Comando ACTIVATE

CLA	‘0C’
INS	‘44’
P1	‘00’
P2	‘00’
Lc	Ausente
Campo de datos	Ausente
Le	Ausente

Tabla 21. Respuesta ACTIVATE

Campo de datos	Ausente
SW1-SW2	Procesamiento normal ‘9000’; Otros valores para indicar errores de comprobación o ejecución *Nota 1.— SW1-SW2 = ‘61XX’ (procesamiento normal) y SW1-SW2 = ‘62XX’ o ‘63XX’ (procedimiento de aviso) quedan fuera del alcance de este documento.*

Después de la ejecución correcta de este comando, el EF.Biometrics actualmente seleccionado DEBE cambiarse al estado activado. En caso de que se produzca un error (SW distinto de ‘9000’), el EF.Biometrics actualmente seleccionado DEBE permanecer en estado desactivado.

Inmediatamente después de la ejecución correcta de este comando (SW1-SW2 = ‘9000’), la autorización efectiva exigida para realizar una acción en el EF.Biometrics DEBE ser la correspondiente al estado activado (con arreglo a la tabla 98). La autorización efectiva correspondiente al estado desactivado NO DEBE suponer ningún derecho de acceso al EF.Biometrics.

3.8.3 Comando FILE AND MEMORY MANAGEMENT

El comando FILE AND MEMORY MANAGEMENT (FMM) inicia una consulta del tamaño de la memoria utilizada o libre del EF direccionado. Este comando se proporciona para la LDS2 del eMRTD como propio. Puede usarse para comprobar el espacio libre disponible del EF direccionado antes de escribir o añadir algo. Asimismo, puede usarse para conseguir el último número de registro añadido para la lectura. P1 indica el método para el direccionamiento de los EF; puede usarse el EF actual o el DO’51’ de referencia del fichero. P2 indica el contenido de la consulta. Se proporcionan el número total de bytes en el EF direccionado con una estructura transparente o de registro y el número de registros existentes o restantes para el EF del registro direccionado. El número total de bytes comprende los bytes disponibles en el EF sin ninguna información estructural. Este número excluye toda información estructural que pueda requerir la LDS2 de la microplaqueta del eMRTD. Para los registros restantes se da por supuesto que su tamaño es el máximo. Después de que el comando FMM se ejecute correctamente, el EF de referencia se convierte en el EF actual.

Tabla 22. Comando FILE AND MEMORY MANAGEMENT (FMM)

CLA	‘8C’	
INS	‘5F’	
P1	Véase la tabla 23	
P2	Véase la tabla 24	
Lc	Ausente para la codificación Nc = 0, presente para la codificación Nc > 0	
Campo de datos	P1 = ‘00’	Ausente
	P1 = ‘01’	DO’51’ de referencia de fichero (véase [ISO/IEC 7816-4])
Le	‘00’	

P1 especifica el método de selección del EF. P2 contiene un mapa de bits que especifica qué información DEBE incluirse en la respuesta.

Tabla 23. Codificación de P1 en el comando FFM

b8	b7	b6	b5	b4	b3	b2	b1	Significado
0	0	0	0	0	0	0	0	EF actual
0	0	0	0	0	0	0	1	DO'51' de referencia de fichero del campo de datos del comando
Cualquier otro valor es RFU.								

Tabla 24. Codificación de P2 en el comando FFM

b8	b7	b6	b5	b4	b3	b2	b1	Significado
-	-	-	-	-	-	-	1	Número total de bytes en el EF direccionado
-	-	-	-	-	-	1	-	Número de registros restantes en el EF del registro direccionado
-	-	-	-	-	1	-	-	Número de registros existentes en el EF del registro direccionado
x	x	x	x	x	-	-	-	00000 (Cualquier otro valor es RFU)
Cualquier otro valor es RFU.								

Tabla 25. Codificación del DO'51' en el campo de datos del comando FMM

Rótulo	Longitud	Valor
'51'	1	Identificador EF breve (bits b8 a b4 codifican un número del 1 al 30; los bits b3 a b1 se ponen en 000)
	2	Identificador de archivo

La respuesta para el comando FMM contiene un conjunto de DO que representan la información solicitada sobre el fichero y el tamaño de la memoria.

Tabla 26. Respuesta para el comando FMM

Campo de datos	Ausente o información sobre el control con arreglo a P2. Véase la tabla 27.
SW1-SW2	'9000', errores de comprobación o ejecución según la norma [ISO/IEC 7816-4]

Tabla 27. Gestión de ficheros y memoria

<table>
<tr><th>Rótulo</th><th>Longitud</th><th colspan="3">Valor</th></tr>
<tr><td rowspan="4">‘7F78’</td><td rowspan="4">Var</td><td colspan="3">DO de File and memory management</td></tr>
<tr><td>Rótulo</td><td>Longitud</td><td>Valor</td></tr>
<tr><td>‘81’</td><td>Var</td><td>Número total de bytes en el EF direccionado</td></tr>
<tr><td>‘82’</td><td>Var</td><td>Número de registros restantes en el EF del registro direccionado</td></tr>
<tr><td>‘83’</td><td>Var</td><td>Número de registros restantes en el EF del registro direccionado</td></tr>
</table>

Nota 1.— La LDS2 de la microplaqueta del eMRTD DEBE devolver solo los objetos de datos del DO del FMM que se soliciten por medio del P2.

Nota 2.— Los datos de respuesta del FMM son válidos únicamente para el EF especificado. Los datos de respuesta del FMM de diferentes EF pueden no ser independientes, p. ej., si diferentes EF comparten la memoria disponible. El IS debería tener esto en cuenta si combina datos de respuesta del FMM de diferentes EF.

Nota 3.— Cuando se aplica la mensajería segura al comando FMM, DEBE usarse el DO’85’ de mensajería segura para encapsular los datos del comando cifrado.

3.9 Especificaciones sobre estructuras de ficheros

La información en la LDS2 de un eMRTD se almacena en un sistema de ficheros definido en [ISO/IEC 7816-4]. El sistema de ficheros se organiza en forma jerárquica en ficheros especializados (DF) y ficheros elementales (EF). Los DF contienen EF u otros ficheros especializados. Un fichero maestro (MF) opcional puede estar en el origen del sistema de ficheros.

Nota.— La necesidad de contar con un fichero maestro se determina por la elección de sistemas de operación, aplicaciones de la LDS1 o LDS2, y condiciones de acceso opcionales.

3.9.1 Codificación de datos

Para los elementos de datos se permiten los tipos de codificación siguientes:

A = Carácter alfabético [a-z, A-Z];
N = Carácter numérico [0-9];
S = Carácter especial [‘<’];
B = Datos binarios;
U = Caracteres UNICODE codificados en UTF-8.

Codificación en UTF-8 de los caracteres UNICODE:

- Para todo carácter igual o inferior a 127 (hex ‘7F’), la codificación en UTF-8 usa un byte que es el mismo que el valor ASCII;

- Para todo carácter igual o inferior a 2 047 (hex ‘07FF’), la codificación en UTF-8 usa dos bytes;
  - el primer byte tiene dos bits de mayor peso fijados y el tercer bit despejado (i. e. hex ‘C2’ a ‘DF’);
  - el segundo byte tiene el bit de mayor peso fijado y el segundo bit despejado (i. e. ‘80’ a ‘BF’);
- Para todos los caracteres iguales o superiores a 2 048 y menores de 65 535 (hex ‘FFFF’), la codificación en UTF-8 usa tres bytes.

3.10 Selección de aplicación — DF

Los eMRTD APOYARÁN por lo menos una aplicación, como sigue:

- La aplicación de la LDS1 para el eMRTD es OBLIGATORIA;
  - la aplicación de la LDS1 para el eMRTD CONSISTIRÁ en los datos registrados por el Estado expedidor u organización expedidora, grupos de datos 1 a 16 conjuntamente con el objeto de seguridad de documento ($EF.SO_D$);
  - el objeto de seguridad de documento ($EF.SO_D$) que se halla dentro de la aplicación de la LDS1 para el eMRTD consiste en las condensaciones que se definen en el Doc 9303-11 y en el Doc 9303-12 para los grupos de datos que se utilicen y se necesiten para validar la integridad de los datos creados por el expedidor y almacenados en la aplicación de la LDS1 para el eMRTD.
- La aplicación de la LDS1 del eMRTD PUEDE, opcionalmente, admitir las aplicaciones de la LDS2 adicionales descritas en el Doc 9303 como:
  - aplicación de los registros de viaje;
  - aplicación de los registros de visados; y
  - aplicación de los datos biométricos adicionales.

Además, los Estados u organizaciones expedidores pueden añadir otras aplicaciones. La estructura de fichero HARÁ lugar a tales aplicaciones adicionales, pero los detalles concretos de las mismas caen fuera del alcance del Doc 9303.

Las aplicaciones de la LDS1 y LDS2 SE SELECCIONARÁN utilizando la identificación de aplicación (AID) como nombre DF reservado. La AID CONSISTIRÁ en el identificador de aplicación registrado asignado por la ISO con arreglo a [ISO/IEC 7816-5] y una extensión de identificador de aplicación de propiedad (PIX) según se especifica en este documento:

En el contexto de la aplicación de la LDS1 para el eMRTD se usan dos sistemas diferentes de asignación de rótulos para el rótulo de la clase de aplicación, según se define en el Doc 9303-10 (rótulo para LDS) y [ISO/IEC 7816-6] (rótulo interindustrial):

- EF.ATR/INFO y EF.DIR usan el sistema de asignación de rótulos interindustriales;
- Los DF y sus EF usan el sistema de asignación de rótulos para LDS.

Los rótulos interindustriales especificados en este documento se usan en el contexto de la LDS, por lo que no es necesario un sistema de asignación de rótulos coexistentes.

3.11 Ficheros elementales comunes (EF)

En el MF PUEDEN existir los siguientes EF comunes para las aplicaciones de la LDS1 y LDS2:

- EF.ATR/INFO;
- EF.DIR;
- EF.CardAccess; y
- EF.CardSecurity.

3.11.1 EF.ATR/INFO (CONDICIONAL)

EF.ATR/INFO es un EF transparente contenido en el fichero maestro y SE EXIGE en forma condicional si la aplicación de la LDS2 opcional está presente. Este EF es opcional si solo está presente la aplicación de la LDS1. El identificador EF breve al nivel del MF es '01'.

Tabla 28. EF.ATR/INFO

Nombre del fichero	EF.ATR/INFO
ID del fichero	'2F01'
Identificador EF breve	'01'
Seleccionar acceso	SIEMPRE
Acceso de lectura	SIEMPRE
Acceso de escritura/actualización /borrado	NUNCA
Estructura del fichero	Transparente
Tamaño	Variable

El contenido del EF.ATR/INFO puede recuperarse utilizando el comando SELECT seguido por el comando READ BINARY. El campo de datos de respuesta para el comando READ BINARY abarca el contenido del EF.ATR/INFO.

Tabla 29. Elementos de datos del EF.ATR/INFO para la LDS2

<table>
<tr><th>Rótulo</th><th>Longitud</th><th colspan="3">Valor</th><th>Notas</th></tr>
<tr><td rowspan="5">‘47’</td><td rowspan="5">‘03’</td><td colspan="3">Capacidad de la tarjeta</td><td></td></tr>
<tr><td colspan="3">byte 1 – primera función del soporte lógico</td><td>b8 = 1: selección del DF por el nombre completo del DF
b7 a b4 y b1 quedan fuera del alcance del Doc 9303 b3 = 1: identificador EF breve admitido
b2 = 1: número de registro admitido</td></tr>
<tr><td colspan="3">byte 2 – segunda función del soporte lógico</td><td>b8, b7, b6 y b5 quedan fuera del alcance del Doc 9303
b4 a b1 = 0001: tamaño de la unidad de datos de 1 byte</td></tr>
<tr><td colspan="3">byte 3 – tercera función del soporte lógico</td><td>b8 = 1: encadenamiento de comandos admitido
b7 = 1: se admiten los campos Lc y Le ampliados
b6 = 1: Información sobre la longitud ampliada en EF.ATR/INFO
b5 a b1 quedan fuera del alcance del Doc 9303</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="4">‘7F66’</td><td rowspan="4">Var</td><td colspan="4">Información sobre la longitud ampliada</td></tr>
<tr><td>Rótulo</td><td>Longitud</td><td>Valor</td><td>Notas</td></tr>
<tr><td>‘02’</td><td>Variable</td><td>Número entero positivo – número máximo de bytes en un comando APDU</td><td>DEBE ser al menos 1 000 (decimal) para la LDS2</td></tr>
<tr><td>‘02’</td><td>Variable</td><td>Número entero positivo – número máximo de bytes esperado en una respuesta APDU</td><td>DEBE ser al menos 1 000 (decimal) para la LDS2</td></tr>
</table>

Nota 1.— Otros objetos de datos PUEDEN estar presentes en EF.ATR/INFO.

Nota 2.— EF.ATR/INFO usa el sistema de asignación de rótulos interindustriales definido en [ISO/IEC 7816-4].

3.11.2 EF.DIR (CONDICIONAL)

EF.DIR es un EF transparente contenido en el fichero maestro definido en [ISO/IEC 7816-4]. EF.DIR SE EXIGE en forma condicional si están presentes algunas aplicaciones de la LDS2 opcionales. Si están presentes algunas aplicaciones de la LDS2 opcionales, DEBE incluirse EF.DIR MUST en SecurityInfos presentes en EF.CardSecurity. Puede encontrarse una descripción completa de SecurityInfo para EF.DIR en el Doc 9303-11.
El identificador EF breve en el MF es ‘1E’.

Tabla 30. EF.DIR

Nombre del fichero	EF.DIR
ID del fichero	‘2F00’
Identificador EF breve	‘1E’
Seleccionar acceso	SIEMPRE
Acceso de lectura	SIEMPRE
Acceso de escritura/actualización /borrado	NUNCA
Estructura del fichero	Transparente
Tamaño	Variable

SE RECOMIENDA que EF.DIR esté presente en el MF. EF.DIR DEBE estar presente si están presentes otras aplicaciones además de la aplicación de la LDS1 obligatoria e indicar las aplicaciones admitidas por el eMRTD. DEBE contener un conjunto de plantillas de aplicaciones que contengan un DO de identificador de aplicación en cualquier orden.

Tabla 31. Formato EF.DIR

<table>
<tr><th>Rótulo</th><th>L</th><th colspan="3">Valor</th><th>Descripción</th></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>Plantilla para la aplicación de la LDS1 del eMRTD</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Rótulo</td><td>L</td><td>Valor</td><td rowspan="2">AID internacional para la aplicación de la LDS1 del eMRTD: ‘A0 00 00 02 47 10 01’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 10 01’</td></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>Plantilla para la aplicación de los registros de viaje</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Rótulo</td><td>L</td><td>Valor</td><td rowspan="2">AID internacional para los registros de viaje: ‘A0 00 00 02 47 20 01’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 20 01’</td></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>Plantilla para la aplicación de los registros de visados</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Rótulo</td><td>L</td><td>Valor</td><td rowspan="2">AID internacional para los registros de visados: ‘A0 00 00 02 47 20 02’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 20 02’</td></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>Plantilla para la aplicación de los datos biométricos adicionales</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Rótulo</td><td>L</td><td>Valor</td><td rowspan="2">AID internacional para la aplicación de los datos biométricos adicionales: ‘A0 00 00 02 47 20 03’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 20 03’</td></tr>
</table>

Nota.— EF.DIR usa el sistema de asignación de rótulos estándar definido en [ISO/IEC 7816-4].

3.11.3 EF.CardAccess (CONDICIONAL)

EF.CardAccess es un EF transparente contenido en el fichero maestro y SE EXIGE de forma condicional si se invoca el control de acceso PACE opcional definido en el Doc 9303-11. Puede encontrarse una descripción completa de SecurityInfo para el PACE en el Doc Doc 9303-11.

El identificador EF breve en el MF es '1C'.

Tabla 32. EF.CardAccess

Nombre del fichero	EF.CardAccess
ID del fichero	'011C'
Identificador EF breve	'1C'
Seleccionar acceso	SIEMPRE
Acceso de lectura	SIEMPRE
Acceso de escritura/actualización/borrado	NUNCA
Estructura del fichero	Transparente
Tamaño	Variable

El file CardAccess contenido en el fichero maestro SE EXIGE si la microplaqueta admite el PACE y CONTENDRÁ las siguientes SecurityInfos que se requieren para el PACE:

- `PACEInfo`;
- `PACEDomainParameterInfo`.

Tabla 33. Almacenamiento de EF.CardAccess en el IC

Nombre del fichero	EF.CardAccess
ID del fichero	'011C'
Identificador EF breve	'1C'
Acceso de lectura	SIEMPRE
Acceso de escritura	NUNCA
Tamaño	Variable
Contenido	SecurityInfos codificadas con DER. Véase el Doc 9303-11.

3.11.4 EF.CardSecurity (CONDICIONAL)

EF.CardSecurity es un EF transparente contenido en el fichero maestro y SE EXIGE de forma condicional si se invoca el PACE opcional con correspondencia de autenticación de microplaqueta según se define en el Doc 9303-11. Puede encontrarse una descripción completa de SecurityInfos para el PACE con correspondencia de autenticación de microplaqueta en el Doc 9303-11.

El identificador EF breve al nivel del MF es '1D'.

El EF.CardSecurity contenido en el MF SE EXIGE si:

- el PACE con correspondencia de autenticación de microplaqueta es admitido por el IC;
- la autenticación del terminal en el MF es admitida por el IC; o
- la autenticación de la microplaqueta en el MF es admitida por el IC.

Y DEBE contener:

- la ChipAuthenticationInfo requerida por la autenticación de la microplaqueta;
- la ChipAuthenticationPublicKeyInfo requerida por el PACE-CAM/autenticación de la microplaqueta;
- la TerminalAuthenticationInfo requerida por la autenticación del terminal;
- las SecurityInfos contenidas en EF.CardAccess.

El fichero EF.CardSecurity contenido en el fichero maestro SE EXIGE si el PACE con correspondencia de autenticación de microplaqueta es admitido por la microplaqueta del eMRTD y CONTENDRÁ las siguientes SecurityInfos:

- la ChipAuthenticationPublicKeyInfo requerida por el PACE-CAM;
- las SecurityInfos contenidas en CardAccess.

Tabla 34. Almacenamiento de EF.CardSecurity en el IC

Nombre del fichero	EF.CardSecurity
ID del fichero	'011D'
Identificador EF breve	'1D'
Acceso de lectura	PACE
Acceso de escritura	NUNCA
Tamaño	Variable

El archivo CardSecurity SE IMPLEMENTARÁ como SignedData con arreglo al [RFC 3369] con el tipo de contenido id-SecurityObject dentro del campo encapContentInfo. El firmante de documentos FIRMARÁ los objetos de seguridad. El certificado de firmante del documento DEBE incluirse en SignedData. El siguiente identificador de objetos SE UTILIZARÁ para identificar el tipo de contenido:

```
bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}
id-SecurityObject OBJECT IDENTIFIER ::= {
    bsi-de applications(3) eID(2) 1
}
```

La estructura de datos SignedData se define de la siguiente manera:

```
SignedData ::= SEQUENCE{
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
    signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

EncapsulatedContentInfo ::= SEQUENCE {
    eContentType ContentType,
    eContent [0] EXPLICIT OCTET STRING OPTIONAL
}

ContentType ::= OBJECT IDENTIFIER

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgoritm SignatureAlgorithmIdentifier,
    signature SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}

SignerIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier
}

SignatureValue ::= OCTET STRING
```

4. APLICACIÓN DE LA LDS1 PARA EL eMRTD (OBLIGATORIA)

La estructura LDS1 para el eMRTD proporciona espacio para almacenar y firmar en forma digital los elementos de datos obligatorios y opcionales que pueden usarse para vincular la persona titular al documento. La información almacenada en la LDS1 del eMRTD se vuelve estática en el momento de expedición y no puede modificarse de ninguna manera. Esta característica es necesaria para proteger la información personal y para que pueda detectarse más fácilmente la manipulación de documentos. Si bien la versión LDS1 del eMRTD incluye campos de datos opcionales que podrían usarse para ampliar el uso del eMRTD (i. e. datos biométricos adicionales, trámites fronterizos automatizados, etc.), el requisito de proteger la aplicación de la LDS1 presente en la microplaqueta del eMRTD contra la escritura en el momento de expedición es OBLIGATORIO.

4.1 Selección de aplicación — DF

La aplicación de la LDS1 para el eMRTD SE SELECCIONARÁ utilizando la identificación de aplicación (AID) como nombre de DF reservado. La AID CONSISTIRÁ en el identificador de aplicación registrado asignado por la ISO con arreglo a [ISO/IEC 7816-5] y una extensión de identificador de aplicación de propiedad (PIX) especificada en este documento:

- el identificador de aplicación registrado es ‘A000000247’;
- la aplicación de datos almacenados por el expedidor UTILIZARÁ PIX = ‘1001’;
- la AID completa de la aplicación de la LDS1 para el eMRTD es ‘A0 00 00 02 47 10 01’.

El CI DEBE rechazar la selección de una aplicación si la extensión de esa aplicación está ausente.

4.2 Plan de ordenamiento aleatorio

El plan de ordenamiento aleatorio permite registrar los grupos de datos y los elementos de datos siguiendo un orden aleatorio compatible con la posibilidad de la tecnología de ampliación de capacidad opcional, que permite la recuperación directa de elementos de datos específicos, incluso si se han registrado fuera de orden. Los elementos de datos de longitud variable se codifican como objetos de datos TLV especificados en ASN.1.

4.3 Representación del fichero de acceso aleatorio

La representación del fichero de acceso aleatorio se ha definido sobre la base de las siguientes consideraciones e hipótesis.

Para apoyar una amplia gama de implementaciones, la LDS comprende una gran variedad de elementos de datos opcionales. Estos elementos de datos se incluyen para facilitar la autenticación de la LDS1 del eMRTD y de la persona titular legítima y para acelerar el procesamiento en los distintos puntos de control de los documentos y personas.

La estructura de datos debe admitir:

- un conjunto limitado o amplio de elementos de datos;
- ocurrencias múltiples de elementos de datos específicos;
- la evolución continua de las implementaciones específicas.

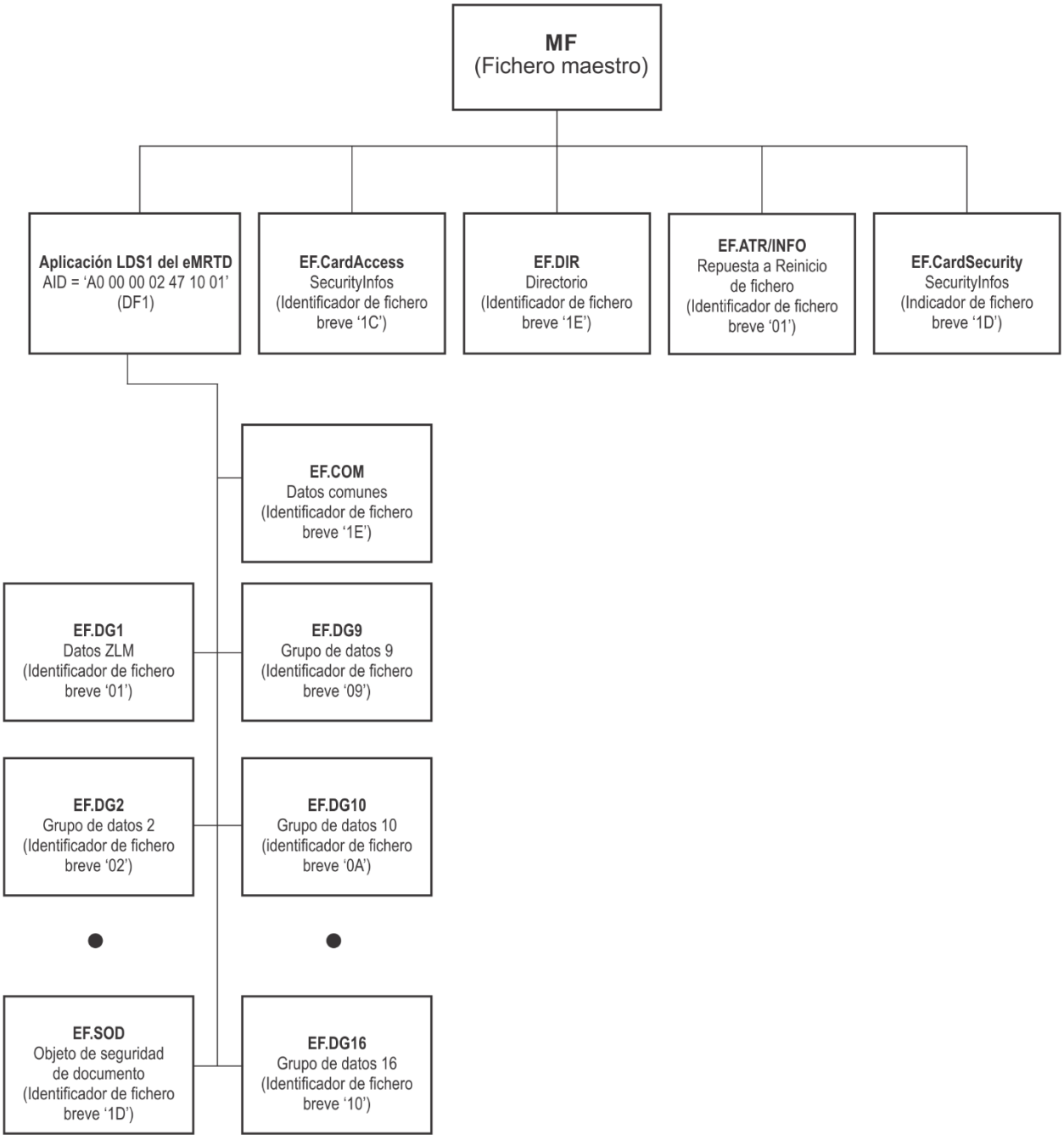


Figura 3. Resumen de la estructura de fichero de la LDS1 del eMRTD

- el apoyo como mínimo a un conjunto de datos de aplicación;
- la posibilidad de otras aplicaciones específicas nacionales;
- el apoyo a la autenticación activa opcional del documento por medio de un par de claves asimétricas almacenadas;
- el apoyo al acceso rápido a elementos de datos seleccionados para facilitar el rápido procesamiento del documento;
- el acceso inmediato a los elementos de datos necesarios; y
- el acceso directo a las plantillas de datos y a los datos biométricos.

4.4 Agrupamiento de los elementos de datos

En una LDS pueden estar presentes o no agrupamientos de elementos de datos añadidos por los Estados expedidores u organizaciones receptoras aprobadas. En la LDS puede estar presente más de un registro de elementos de datos agrupados añadidos por los Estados receptores u organizaciones receptoras aprobadas.

La capacidad de un Estado receptor u organización receptora aprobada para añadir datos a la LDS no se considera en esta edición del Doc 9303.

La LDS se considera una entidad cohesiva única que contiene el número de agrupamientos de elementos de datos registrados en la tecnología de ampliación de capacidad opcional en el momento de efectuarse la lectura mecánica.

La LDS se ha diseñado con la flexibilidad suficiente para que pueda aplicarse a todos los tipos de eMRTD. En las figuras y tablas que siguen, algunos elementos de datos solo se aplican a los visados de lectura mecánica y a los pasaportes de lectura mecánica, o exigen una presentación diferente para dichos documentos.

Dentro de la LDS se han establecido agrupamientos lógicos de elementos de datos conexos. Estos agrupamientos lógicos se conocen como grupos de datos.

4.5 Requisitos de la estructura lógica de datos

La tecnología de ampliación de capacidad del CI sin contacto contenida en la LDS1 de un eMRTD seleccionada por un Estado expedidor u organización expedidora debe permitir que los Estados receptores tengan acceso a los datos correspondientes.

La OACI ha determinado que la estructura lógica de datos (LDS) predefinida y normalizada DEBE satisfacer varios requisitos obligatorios:

- asegurar la facilitación eficiente y óptima de la persona titular legítima;
- asegurar la protección de los detalles registrados en la tecnología de ampliación de la capacidad opcional;
- permitir la interoperabilidad mundial de los datos de capacidad ampliada basándose en el uso de una LDS única común a todos los eMRTDs;

- responder a las diversas necesidades de ampliación de capacidad opcional de los Estados expedidores y las organizaciones expedidoras;
- proporcionar ampliación de capacidad a medida que evolucionan las necesidades de las personas usuarias y la tecnología disponible
- permitir una variedad de opciones de protección de datos;
- utilizar las especificaciones internacionales existentes en la mayor medida posible, en particular las especificaciones internacionales emergentes para una biometría interoperable a escala mundial.

4.5.1 Seguridad

Solo el Estado expedidor u organización expedidora TENDRÁ acceso de escritura a estos grupos de datos. Por consiguiente, no hay requisitos de intercambio y los métodos para lograr la protección contra la escritura no forman parte de esta especificación. Una vez bloqueada la microplaqueta (después de la personalización y antes de la expedición) no pueden escribirse, modificarse ni suprimirse datos de la aplicación de la LDS1 en/de la microplaqueta. Después de la expedición, las microplaquetas bloqueadas no pueden desbloquearse.

4.5.2 Autenticidad e integridad de los datos

Para permitir la confirmación de la autenticidad e integridad de los detalles registrados, se incluye un objeto de autenticidad/integridad. Cada grupo de datos DEBE estar representado en este objeto de autenticidad/integridad, que se registra en un fichero elemental EF separado (EF.SOD). Empleando la estructura de marco común de formatos de intercambio biométrico (CBEFF) utilizada para los grupos de datos 2-4 de las características de identificación codificadas y las características opcionales de “seguridad biométrica adicional” definidas en el Doc 9303-12, también PUEDEN protegerse individualmente los elementos de confirmación de la identidad (p. ej., las plantillas biométricas) a discreción del Estado expedidor o de la organización expedidora.

4.5.3 Ordenamiento de la LDS

Para la interoperabilidad internacional solo SE UTILIZARÁ el plan de ordenamiento aleatorio.

4.5.4 Capacidad de almacenamiento de datos del CI sin contacto

La capacidad de almacenamiento de datos del CI sin contacto queda a la discreción del Estado expedidor, pero SERÁ de un mínimo de 32 kB. Esta capacidad mínima es necesaria para almacenar la imagen facial obligatoria, los datos de la ZLM y los elementos necesarios para asegurar los datos. El almacenamiento de imágenes faciales adicionales, de huellas digitales y/o del iris puede exigir un aumento considerable de la capacidad de almacenamiento de datos. No hay un valor máximo especificado de la capacidad de datos del CI sin contacto.

En caso de que la infraestructura PKI de un Estado no esté disponible para firmar los datos de la LDS1 para el eMRTD como parte de la personalización y no pueda postergarse la expedición del/de los documento(s), SE RECOMIENDA que el CI sin contacto de la LDS1 para el eMRTD se deje en blanco y se bloquee. La LDS1 para el El eMRTD DEBERÍA contener una aprobación adecuada al respecto. Se prevé que esto constituya una circunstancia excepcional.

4.5.5 Almacenamiento de otros datos

Un Estado PUEDE utilizar la capacidad de almacenamiento del CI sin contacto en un eMRTD para ampliar la capacidad de datos de lectura mecánica de la LDS1 para el eMRTD más allá de la definida para la interoperabilidad mundial. Esto puede tener la finalidad de proporcionar acceso de lectura mecánica a información de documentos de identidad (p. ej., detalles del certificado de nacimiento), a elementos de confirmación de la identidad personal almacenada (elementos biométricos) y/o a detalles de verificación de la autenticidad del documento.

4.5.6 Norma internacional para la codificación biométrica

La norma ISO/IEC 39794 sustituyó a la norma [ISO/IEC 19794:2005] como norma internacional para la codificación biométrica. Se ha definido el siguiente calendario de transición:

- el 1/1/2025, una vez transcurrido el período de preparación de cinco años iniciado el 1/1/2020, los equipos de lectura de pasaportes DEBEN estar en condiciones de manejar los datos ISO/IEC 39794;
- entre 2025 y 2030 los expedidores de pasaportes pueden emplear los formatos de datos especificados en ISO/IEC 19794-X:2005 o en ISO/IEC 39794-X durante un período de transición de cinco años. Durante este período de transición, serán esenciales la interoperabilidad y las pruebas de conformidad; y
- del 1/1/2030 en adelante, los expedidores de pasaportes DEBEN emplear la ISO/IEC 39794-X para codificar los datos biométricos.

La ISO/IEC 49794 proporciona orientación sobre la transición de la [ISO/IEC 19794:2005] a la ISO/IEC 39794.

4.6 Ficheros elementales (EF) de la LDS1 para eMRTD

4.6.1 Información de presencia de encabezamiento y grupo de datos EF.COM (OBLIGATORIO)

El EF.COM está ubicado en la aplicación de la LDS1 para el eMRTD (identificador de fichero breve = 1E) y contiene información sobre la versión LDS, información sobre la versión de Unicode y una lista de los grupos de datos que están presentes en la aplicación. La aplicación de la LDS1 para el eMRTD DEBE tener solamente un fichero EF.COM que contenga la información común para la aplicación.

Los elementos de datos que pueden figurar en esta plantilla son los siguientes:

Tabla 35. Rótulos normativos de EF.COM

Rótulo	**L**	**Valor**		
‘60’	Var	Información del nivel de la aplicación		
		Rótulo	**L**	**Valor**
		‘5F01’	‘04’	Número de versión LDS con formato aabb, donde aa define la versión de la LDS y bb define el nivel de actualización.
		‘5F36’	‘06’	Número de versión Unicode con formato aabbcc, donde aa define la versión principal, bb define la versión menor y cc define el nivel de difusión.
		‘5C’	Var	Lista de rótulos. Lista de todos los grupos de datos presentes.

Se INCLUIRÁ un encabezamiento y un mapa de presencia de grupos de datos. El encabezamiento CONTENDRÁ la información siguiente, que permite al Estado receptor u organización receptora aprobada ubicar y descodificar los diversos grupos de datos y elementos de datos contenidos dentro del bloque registrado por el Estado expedidor u organización expedidora.

Se RECOMIENDA que los sistemas de inspección que dependen del EF.COM se modifiquen para utilizar el SO_D descrito en la versión 1.8 de LDS tan pronto como sea posible.

4.6.1.1 Número de versión LDS

El número de versión LDS define la versión de formato de la LDS. El formato exacto que ha de utilizarse para almacenar este valor se define en la sección 4.6 del presente documento. El formato normalizado para un número de versión LDS es “aabb”, donde:

- “aa” = número (01-99) que identifica la versión principal de la LDS (es decir, adiciones significativas a la LDS);
- “bb” = número (01-99) que identifica la versión menor de la LDS.

4.6.1.2 Número de versión UNICODE

El número de versión Unicode identifica el método de codificación utilizado cuando se registran caracteres alfabéticos, numéricos y especiales, incluso caracteres nacionales. El formato exacto que ha de emplearse para almacenar este valor se define en la sección 4.7.1 de este documento. El formato normalizado para un número de versión Unicode es “aabbcc”:

- “aa” = número que identifica la versión principal de la especificación Unicode (es decir, adiciones significativas a la especificación) publicada como libro;
- “bb” = número que identifica la versión menor de la especificación Unicode (es decir, adiciones de caracteres o más cambios normativos significativos, publicados como informe técnico); y
- “cc” = número que identifica la versión actualizada de la especificación Unicode (es decir, cualquier otro cambio a las partes normativas o informativas importantes de la especificación que podría modificar el comportamiento del programa. Estos cambios se reflejan en nuevos ficheros de bases de datos de caracteres Unicode y en una página de actualización). Por razones históricas, la numeración dentro de cada uno de los campos (es decir, a, b, c) no es necesariamente consecutiva.

El conjunto de caracteres universal (UCS) DEBE cumplir la [ISO/IEC 10646].

4.6.2 Objeto de seguridad del documento $EF.SO_D$ (OBLIGATORIO)

Además de los grupos de datos de LDS, el CI sin contacto contiene un objeto de seguridad de documento almacenado en $EF.SO_D$. Este objeto es firmado digitalmente por el Estado expedidor y contiene valores de condensación del contenido de la LDS.

Tabla 36. Rótulos $EF.SO_D$

Rótulo	L	Valor
‘77’	Var	Objeto de seguridad del documento

Se han desplegado dos versiones del objeto de seguridad del documento EF.SO_D: Se trata de la versión EF.SO_D V0 ya existente, que puede encontrarse en el apéndice D, y de la versión RECOMENDADA EF.SO_D V1, que figura en esta sección. Solo SE EXIGE y permite una EF.SO_D.

4.6.2.1 Objeto de seguridad del documento EF.SOD V1 LDS v1.8

El objeto de seguridad del documento V1 para la LDS v1.8 se ha ampliado con un atributo firmado, que contiene la información sobre la versión de la LDS y la versión Unicode:

```
LDSSecurityObject ::= SEQUENCE {
    version LDSSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash,
    ldsVersionInfo LDSVersionInfo OPTIONAL
    -- Si está presente, la version DEBE ser V1
}
LDSVersionInfo ::= SEQUENCE {
    ldsVersion PrintableString,
    unicodeVersion PrintableString }
```

4.6.2.2 Tipo de datos firmados (SignedData Type) para SO_D V1

El objeto de seguridad del documento se implementa como tipo SignedData, según se especifica en [RFC 3369], Cryptographic Message Syntax (CMS), agosto de 2002. Todos los objetos de seguridad DEBEN producirse en formato de regla de codificación distinguida (DER) para preservar la integridad de las firmas que contengan.

Nota 1.— m = EXIGIDO — el campo ESTARÁ presente.

Nota 2.— x= no utilizar — el campo NO DEBERÍA llenarse.

Nota 3.— o = opcional — el campo PUEDE estar presente.

Nota 4.— c = elección — el contenido del campo es una elección entre alternativas.

Tabla 37. Tipo de datos firmados para SO_D V1

Valor		Comentarios
SignedData		
Version	m	Valor = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	El contenido codificado de un ldsSecurityObject.
Certificates	m	SE EXIGE que Los Estados incluyan el certificado de firmante del documento (C_{DS}) que puede utilizarse para verificar la firma en el campo signerInfos.
Crls	x	Se recomienda que los Estados no utilicen este campo.
signerInfos	m	Se recomienda que los Estados solo proporcionen un signerInfo en este campo.

Valor		Comentarios
SignerInfo	m	
Version	m	El valor de este campo está dictado por el campo sid. Véanse las reglas relativas a este campo en RFC 3369, Doc 9303-12.
Sid	m	
issuerandSerialNumber	c	Se recomienda que los Estados apoyen este campo antes que subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	El identificador del algoritmo utilizado para producir el valor condensado por encima de encapsulatedContent y SignedAttrs.
signedAttrs	m	Puede que los Estados productores deseen incluir atributos adicionales para añadir a la firma; no obstante, estos no tienen que ser procesados por los Estados receptores, excepto para verificar el valor de la firma.
signatureAlgorithm	m	El identificador del algoritmo utilizado para producir el valor de firma en cualquier parámetro conexo.
Signature	m	El resultado del proceso de generación de firma.
unsignedAttrs	o	Puede que los Estados productores deseen utilizar este campo, pero no se recomienda y los Estados receptores pueden optar por ignorarlo.

4.6.2.3 ASN.1 Profile LDS Document Security Object for SO_D V1

```
LDSSecurityObjectV1 { joint-iso-itu-t(2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

-- Imports from RFC 3280 [PROFILE]
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) };

-- Constantes

ub-DataGroups INTEGER ::= 16

-- Identificadores de objeto

id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject  OBJECT  IDENTIFIER  ::=  {id-icao-  mrtd-
security 1}
```

```
-- Objeto de seguridad LDS

LDSSecurityObjectVersion ::= INTEGER {v0(0), v1(1)
-- If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present
}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash,
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1
}
DataGroupHash ::= SEQUENCE {
   dataGroupNumber DataGroupNumber,
   dataGroupHashValue OCTET STRING }

DataGroupNumber ::= INTEGER {
   dataGroup1        (1),
   dataGroup2        (2),
   dataGroup3        (3),
   dataGroup4        (4),
   dataGroup5        (5),
   dataGroup6        (6),
   dataGroup7        (7),
   dataGroup8        (8),
   dataGroup9        (9),
   dataGroup10            (10),
   dataGroup11            (11),
   dataGroup12            (12),
   dataGroup13            (13),
   dataGroup14            (14),
   dataGroup15            (15),
   dataGroup16            (16)}

LDSVersionInfo ::= SEQUENCE {
   ldsVersion PrintableString
   unicodeVersion Printable String }
END
```

Nota 1.— El campo `dataGroupHashValue` *contiene la condensación calculada sobre el contenido completo del grupo de datos EF, especificado por* `dataGroupNumber`.

Nota 2.— Los `DigestAlgorithmIdentifiers` *DEBEN omitir los parámetros "NULL", mientras que el* `SignatureAlgorithmIdentifier` *(definido en RFC 3447) DEBE incluir* `NULL` *como parámetro si no hay parámetros presentes, incluso cuando se usen algoritmos SHA2 con arreglo a RFC 5754. El sistema de inspección DEBE aceptar el campo* `DigestAlgorithmIdentifiers` *con ambas condiciones, es decir, parámetros ausentes o parámetros NULL.*

4.7 Elementos de datos que integran los grupos de datos 1 a 16

Los grupos de datos 1 (DG1) a 16 (DG16) consisten cada uno en varios elementos de datos obligatorios, opcionales y condicionales. Se SEGUIRÁ el orden especificado de los elementos de datos dentro del grupo de datos. Cada grupo de datos se ALMACENARÁ en un EF transparente. El direccionamiento de los EF SE HARÁ por identificador de EF breve, como se indica en la Tabla 38. Los EF TENDRÁN nombres de fichero conformes al número n, EF.DGn, donde n es el número del grupo de datos.

Tabla 38. Elementos de datos obligatorios y opcionales que se combinan para formar la estructura de los grupos de datos 1 (DG1) a 16 (DG16)

Grupo de datos	Nombre de EF	Identificador de EF breve	Identificador de EF	Rótulo
Común	EF.COM	‘1E’	‘01 1E’	‘60’
DG1	EF.DG1	‘01’	‘01 01’	‘61’
DG2	EF.DG2	‘02’	‘01 02’	‘75’
DG3	EF.DG3	‘03’	‘01 03’	‘63’
DG4	EF.DG4	‘04’	‘01 04’	‘76’
DG5	EF.DG5	‘05’	‘01 05’	‘65’
DG6	EF.DG6	‘06’	‘01 06’	‘66’
DG7	EF.DG7	‘07’	‘01 07’	‘67’
DG8	EF.DG8	‘08’	‘01 08’	‘68’
DG9	EF.DG9	‘09’	‘01 09’	‘69’
DG10	EF.DG10	‘0A’	‘01 0A’	‘6A’
DG11	EF.DG11	‘0B’	‘01 0B’	‘6B’
DG12	EF.DG12	‘0C’	‘01 0C’	‘6C’
DG13	EF.DG13	‘0D’	‘01 0D’	‘6D’
DG14	EF.DG14	‘0E’	‘01 0E’	‘6E’
DG15	EF.DG15	‘0F’	‘01 0F’	‘6F’
DG16	EF.DG16	‘10’	‘01 10’	‘70’
Objeto de seguridad del documento	EF.SOD	‘1D’	‘01 1D’	‘77’
Común	EF.CARDACCESS	‘1C’	‘01 1C’	
Común	EF.ATR/INFO	‘01’	‘2F 01’	
Común	EF.CardSecurity	‘1D’	‘01 1D’	

4.7.1 GRUPO DE DATOS 1 — Información en la zona de lectura mecánica (OBLIGATORIO)

Los elementos de datos del Grupo de datos 1 (DG1) tienen por objeto reflejar el contenido completo de la zona de lectura mecánica (ZLM) independientemente de si esta contiene datos reales o caracteres de relleno. Los detalles sobre la implementación de la ZLM dependen del tipo de LDS1 DE LA eMRTD (formatos DV1, DV2 o DV3).

Este elemento de datos contiene la información de la ZLM EXIGIDA para el documento en la plantilla '61'. La plantilla contiene un objeto de datos, la ZLM en el objeto de datos '5F1F'. El objeto de datos ZLM es un elemento de datos compuesto, idéntico a la información ZLM OCR-B impresa en el documento.

Tabla 39. Rótulos del grupo de datos 1

Rótulo	**L**	**Valor**		
'61'	Var			
		Rótulo	**L**	**Valor**
		'5F1F'	Var	El objeto de datos ZLM es un elemento de datos compuesto. (EXIGIDO) (El elemento de datos contiene todos los campos obligatorios desde el tipo de documento hasta el dígito de verificación compuesto.)

4.7.1.1 GRUPO DE DATOS 1 – Datos de EF.DG1 para la LDS1 del eMRTD de tamaño DV1

En esta sección se describen los elementos de datos que pueden estar presentes en el grupo de datos 1 (DG1). Los requisitos sobre almacenamiento, ordenamiento y codificación del DG1 son exactamente los mismos que figuran en la ZLM impresa y se describen en las Partes 3 y 5 del Doc 9303-3. Los elementos de datos y sus formatos dentro de cada zona de grupo de datos para DV1 SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], F = campo de longitud fija.

Tabla 40. Elementos de datos para el formato DV1

Elemento de dato	**Opcional u OBLIGATORIO**	**Nombre del elemento de dato**	**Núm. de bytes**	**Fijo o variable**	**Tipo de codificación**
01	M	Código de documento	2	F	A, S
02	M	Estado expedidor u organización expedidora	3	F	A, S
03	M	Número de documento (nueve caracteres más significativos)	9	F	A, N, S

Elemento de dato	Opcional u OBLIGATORIO	Nombre del elemento de dato	Núm. de bytes	Fijo o variable	Tipo de codificación
04	M	Dígito de verificación — Número del documento o carácter de relleno (<) que indica que el número de documento excede de nueve caracteres	1	F	N, S
05	M	Datos opcionales o, en el caso de un número de documento que exceda de nueve caracteres, caracteres menos significativos del número de documento más dígito de verificación del número de documento más carácter de relleno	15	F	A, N, S
06	M	Fecha de nacimiento	6	F	N,S
07	M	Dígito de verificación — Fecha de nacimiento	1	F	N
08	M	Sexo	1	F	A,S
09	M	Fecha de caducidad	6	F	N
10	M	Dígito de verificación — Fecha de caducidad	1	F	N
11	M	Nacionalidad	3	F	A,S
12	M	Datos opcionales	11	F	A,N,S
13	M	Dígito de verificación compuesto	1	F	N
14	M	Nombre del titular	30	F	A,N,S

4.7.1.2 GRUPO DE DATOS 1 — Elementos de datos de EF.DG1 para eMRTD de tamaño DV2

En esta sección se describen los elementos de datos que pueden estar presentes en el grupo de datos 1 (DG1). Los requisitos de almacenamiento, ordenamiento y codificación del DG1 son exactamente los mismos que figuran en la ZLM impresa y se describen en las Partes 3 y 6 del Doc 9303. Los elementos de datos y su formato dentro de cada zona de grupo de datos para DV2 SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], F = campo de longitud fija.

Tabla 41. Elementos de datos para el formato DV2

Dato	Opcional u OBLIGATORIO	Nombre del elemento de dato	Núm. de bytes	Fijo o variable	Tipo de codificación
01	M	Número documento	2	F	A, S
02	M	Estado expedidor u organización expedidora	3	F	A, S
03	M	Nombre del titular	31	F	A, N, S
04	M	Número de documento (nueve caracteres principales)	9	F	A, N, S
05	M	Dígito de verificación	1	F	N, S
06	M	Nacionalidad	3	F	A, S
07	M	Fecha de nacimiento	6	F	N, S
08	M	Dígito de verificación	1	F	N
09	M	Sexo	1	F	A, S
10	M	Fecha de caducidad	6	F	N
11	M	Dígito de verificación	1	F	N
12	M	Datos opcionales más carácter de relleno	7	F	A, N, S
13	M	Dígito de verificación compuesto - ZLM línea 2	1	F	N

4.7.1.3 GRUPO DE DATOS 1 — Datos de EF.DG1 para la LDS1 de eMRTD de tamaño DV3

En esta sección se describen los elementos de datos que pueden estar presentes en el grupo de datos 1 (DG1). Los requisitos de almacenamiento, ordenamiento y codificación del DG1 son exactamente los mismos que figuran en la ZLM impresa y se describen en las Partes 3 y 4 del Doc 9303. Los elementos de datos y su formato dentro de cada zona de grupo de datos para DV3 SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], F = campo de longitud fija.

Tabla 42. Elementos de datos para el formato DV3

Dato	Opcional u OBLIGATORIO	Nombre del dato	Número de bytes	Fijo o variable	Tipo de codificación
01	M	Tipo de documento	2	F	A, S
02	M	Estado expedidor u organización expedidora	3	F	A, S
03	M	Nombre del titular	39	F	A, S
04	M	Número de documento	9	F	A, N, S
05	M	Dígito de verificación — Núm. de documento	1	F	N, S
06	M	Nacionalidad	3	F	A, S
07	M	Fecha de nacimiento	6	F	N, S
08	M	Dígito de verificación — Fecha de nacimiento	1	F	N
09	M	Sexo	1	F	A, S
10	M	Fecha de caducidad	6	F	N
11	M	Dígito de verificación — Fecha de caducidad o válido hasta	1	F	N
12	M	Datos opcionales	14	F	A, N, S
13	M	Dígito de verificación	1	F	N
14	M	Dígito de verificación compuesto	1	F	N

4.7.2 GRUPO DE DATOS 2 — Elementos de identificación codificados — Rostro (OBLIGATORIO)

El grupo de datos 2 (DG2) representa la característica biométrica de interfuncionamiento mundial para la confirmación mecánica de identidad con documentos de viaje de lectura mecánica, que CONSISTIRÁ en una imagen facial del titular como elemento de entrada a un sistema de reconocimiento del rostro. Si existe más de un registro, la primera entrada SERÁ la codificación de interfuncionamiento internacional más reciente.

Tabla 43. Rótulos del grupo de datos 2

Rótulo	L	Valor
‘75’	Var	Véase la codificación biométrica del EF.DG2

4.7.2.1 Codificación biométrica del EF.DG2

El DG2 DEBE utilizar la plantilla de grupo de plantillas de información biométrica (BIT) con los BIT anidados que se especifican en [ISO/IEC 7816-11], para tener la posibilidad de almacenar múltiples plantillas biométricas, que se correspondan con el CBEFF. El subencabezamiento biométrico define el tipo de característica biométrica presente y la característica biométrica específica. La opción anidada de ISO/IEC [7816-11] ha de utilizarse siempre, incluso para codificaciones de una única plantilla biométrica. Este último caso se indica numerando con n = 1.

Cada plantilla anidada tiene la estructura siguiente:

Tabla 44. Grupo de datos 2 — Rótulos de codificación biométrica

Rótulo	**L**	**Valor**				
‘7F61’	Var	Plantilla de grupo de la plantilla de información biométrica				
		Rótulo	**L**	**Valor**		
		‘02’	‘01’	Entero — Número de casos de este tipo de característica biométrica		
		‘7F60’	Var	Primera plantilla de información biométrica		
			Rótulo	**L**		
			‘A1’	Var	Plantilla de encabezamiento biométrico (BHT)	
				Rótulo	**L**	**Valor**
				‘80’	‘02’	Versión 0101 del encabezamiento de la OACI (opcional) — Versión del formato de encabezamiento patrón CBEFF
				‘81’	‘01-03’	Tipo de característica biométrica (opcional)
				‘82’	‘01’	Subtipo de característica biométrica opcional para DG2
				‘83’	‘07’	Fecha y hora de creación (opcional)
				‘85’	‘08’	Período de validez (desde-hasta) (opcional)
				‘86’	‘04’	Creador del dato de referencia biométrica (PID) (opcional)
				‘87’	‘02’	Propietario del formato (EXIGIDO)
				‘88’	‘02’	Tipo de formato (EXIGIDO)
			‘5F2E’ o ‘7F2E’	Var	Los datos biométricos (codificados con arreglo al propietario del formato) también se denominan bloque de datos biométricos (BDB).	

Se utiliza el OID del CBEFF por defecto. El objeto de datos OID (rótulo '06') especificado en la plantilla de información biométrica (BIT, rótulo '7F60') especificado en [ISO/IEC 7816-11] no se incluye en esta estructura. Análogamente, la autoridad de asignación de rótulos no se especifica en la estructura.

Para facilitar la interoperabilidad, la primera característica biométrica registrada en cada grupo de datos se CODIFICARÁ con arreglo a [ISO/IEC19794-5].

Nota.— ISO/IEC 39794 sustituirá a ISO/IEC 19794:2005 como norma internacional para la codificación biométrica. Véase la sección 4.5.6.

4.7.2.2 GRUPO DE DATOS 2 — Datos de EF.DG2

En esta sección se describen los datos que pueden estar presentes en el grupo de datos 2 (DG2). Los elementos de datos y su formato dentro del grupo de datos SERÁN los que se indican en las tablas siguientes:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 45. Elementos de datos para DG2

Elemento de datos	Opcional u OBLIGATORIO	Nombre del elemento de datos	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M	Núm. de codificaciones biométricas del rostro registradas	1	F	N	1 a 9, identificando número de codificaciones únicas de datos del rostro.
02	M	Encabezamiento		Var	A, N	El elemento de datos puede repetirse, según lo definido por el elemento de datos 01.
03	M	Codificaciones de datos biométricos del rostro		Var	A, N, S, B	El dato puede repetirse, según lo definido por el elemento de datos 01.

4.7.3 GRUPO DE DATOS 3 — Elementos de identificación adicionales — Dedos (OPCIONAL)

La OACI reconoce que los Estados miembros pueden optar por utilizar la huella digital o el reconocimiento del iris como tecnologías biométricas adicionales para apoyar la confirmación mecánica de la identidad que SERÁN codificados como grupo de datos 3 (DG3).

Tabla 46. Rótulos del Grupo de datos 3

Rótulo	L	Valor
'63'	Var	Véase la codificación biométrica de EF.DG3

4.7.3.1 Codificación biométrica de EF.DG3

El DG3 DEBE utilizar la plantilla del grupo de plantilla de información biométrica (BIT) con BITS anidadas según se especifica en [ISO/IEC 7816-11], para tener la posibilidad de almacenar múltiples plantillas biométricas, que se correspondan con el CBEFF. El subencabezamiento biométrico define el tipo de característica biométrica presente y la característica biométrica específica. La opción anidada de [ISO/IEC 7816-11] DEBE utilizarse, incluso para codificaciones de una única plantilla biométrica. Este último caso se indica numerando con n = 1. El número de casos en DG3 puede ser '0...n'.

Cada plantilla anidada tiene la estructura siguiente:

Tabla 47. Rótulos anidados del grupo de datos 3

Rótulo	**L**	**Valor**				
'7F61'	Var	Plantilla del grupo de la plantilla de información biométrica				
		Rótulo	**L**	**Valor**		
		'02'	'01'	Entero — Número de casos de este tipo de característica biométrica		
		'7F60'	Var	Primera plantilla de información biométrica		
			Rótulo	**L**		
			'A1'	Var	Plantilla de encabezamiento biométrico (BHT)	
				Rótulo	**L**	**Valor**
				'80'	'02'	Versión '0101'del encabezamiento de la OACI (opcional) — Versión del formato de encabezamiento patrón CBEFF
				'81'	'01-03'	Tipo de característica biométrica (opcional)
				'82'	'01'	Subtipo de característica biométrica EXIGIDO para DG3
				'83'	'07'	Fecha y hora de creación (opcional)
				'85'	'08'	Período de validez (desde hasta) (Oopcional)
				'86'	'02'	Creador del dato de referencia biométrica (PID) (opcional)
				'87'	'02'	Propietario del formato (EXIGIDO)
				'88'	'02'	Tipo de formato (EXIGIDO)
			'5F2E' o '7F2E'	Var	Los datos biométricos (codificados con arreglo al propietario de formato) también se denominan bloques de datos biométricos (BDB).	

Rótulo	**L**	**Valor**				
		Rótulo	**L**			
		‘7F60’	X	Segunda plantilla de información biométrica		
			Rótulo	**L**		
			‘A1’	Var	Plantilla de encabezamiento biométrico (BHT)	
				Rótulo	**L**	**Valor**
				‘80’	‘02’	Versión ‘0101’ del encabezamiento de la OACI (opcional) — Versión del formato de encabezamiento patrón CBEFF
				‘81’	‘01-03’	Tipo de característica biométrica (opcional)
				‘82’	‘01’	Subtipo de característica biométrica EXIGIDO para DG3
				‘83’	‘07’	Fecha y hora de creación (opcional)
				‘85’	‘08’	Período de validez (desde-hasta) (opcional)
				‘86’	‘04’	Creador del dato de referencia biométrica (PID) (opcional)
				‘87’	‘02’	Propietario del formato (EXIGIDO)
				‘88’	‘02’	Tipo del formato (EXIGIDO)
			‘5F2E’ o ‘7F2E’	Var	Los datos biométricos (codificados con arreglo al propietario de formato) también se denominan bloques de datos biométricos (BDB).	

Se utiliza el OID de CBEFF por defecto. El objeto de datos OID (rótulo ‘06’) en la plantilla de información biométrica (BIT, rótulo ‘7F60’) especificado en [ISO/IEC 7816-11] no se incluye en esta estructura. Análogamente, la autoridad de asignación de rótulo no se especifica en la estructura.

Para facilitar la interoperabilidad, la primera característica biométrica registrada en cada grupo de datos SE CODIFICARÁ con arreglo a [ISO/IEC19794-4].

Nota.— ISO/IEC 39794 sustituirá a ISO/IEC 19794:2005 como norma internacional para la codificación biométrica. Véase la sección 4.5.6.

4.7.3.2 GRUPO DE DATOS 3 — Datos de EF.DG3

En esta sección se describen los datos que pueden estar presentes en el Grupo de datos 3 (DG3). Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial [‘<’], B = datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 48. Elementos de datos para DG3

Dato	Opcional u OBLIGATORIO	Nombre del elemento de datos	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M (Si se incluye característica de dedos codificada)	Número de codificaciones biométricas de dedos registradas	1	F	N	0 a n identificando número de codificaciones únicas de datos de dedos.
02	M (Si se incluye característica de dedos codificada)	Encabezamiento		Var	B	El elemento de datos puede repetirse, según se define en el elemento de datos 01.
03	M (Si se incluye característica de dedos codificada)	Codificaciones de datos biométricos de dedos		Var	A, N, S, B	El elemento de datos puede repetirse, según se define en el elemento de datos 01.

4.7.3.2.1 Codificación del subtipo de característica biométrica

Los rótulos de la plantilla de encabezamiento biométrico y sus valores asignados son los mínimos que cada implementación ADMITIRÁ según se indica en la tabla siguiente. Cada plantilla de información biométrica individual tiene la estructura siguiente:

Tabla 49. Plan para la codificación de subcaracterísticas: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Subtipo de característica biométrica
0	0	0	0	0	0	0	0	Sin información
						0	1	Derecho
						1	0	Izquierdo
			0	**0**	**0**			**Sin significado**
			0	0	1			Pulgar
			0	1	0			Índice
			0	1	1			Medio
			1	0	0			Anular
			1	0	1			Meñique
X	X	X						Reservado para uso futuro

4.7.3.2.2 Codificación de cero casos

Los Estados que no expiden LDS1 para eMRTD con huellas digitales NO DEBERÍAN rellenar el DG3. El DG3 de esta estructura tiene el inconveniente de que resultará en una condensación estática de DG3 en el SO_D para todas las LDS1 de los eMRTD en que los datos biométricos no estén presentes ni introducidas en el momento de expedición de la LDS1del eMRTD, pero se haya declarado el DG3. Para fines de interoperabilidad, los Estados que incluyen huellas digitales en sus LDS1 del eMRTD DEBEN almacenar una plantilla del grupo de información biométrica vacía en los casos en que no se disponga de huella digital en el momento de la expedición de la LDS1 del eMRTD. El contador de la plantilla indica un valor de '00' en este caso.

Se RECOMIENDA añadir el rótulo '53' con un contenido definido por el expedidor (p. ej., un número aleatorio).

Tabla 50. Codificación de cero casos

Rótulo	**L**	**Valor**				
'63'	Var	Elemento LDS				
		Rótulo	**L**	**Valor**		
		'7F 61'	'03'	Plantilla de grupo de información biométrica		
			'02'	'01'	'00'	Define que no hay plantillas de información biométrica almacenadas en este grupo de datos.
		'53'	Var	Contenido definido por el expedidor (p. ej., un número aleatorio).		

4.7.3.2.3 Codificación de un caso

En los casos en que solo se disponga de una huella digital, DEBE codificarse el caso único de la manera siguiente (ejemplo para DG3 – huella digital):

Tabla 51. Codificación de un caso

Rótulo	**L**	**Valor**				
'63'	Var	Elemento LDS donde aa es la longitud total del contenido completo del dato LDS				
		Rótulo	**L**	**Valor**		
		'7F 61'	Var	Plantilla de grupo de información biométrica.		
			'02'	'01'	'01'	Define el número total de huellas digitales almacenadas como plantillas de información biométrica que siguen.

Rótulo	L	Valor						
			‘7F 60’	Var	Primera plantilla de información biométrica donde cc es la longitud total de todos los BIT			
				‘A1’	Var	Plantilla de encabezamiento biométrico		
					‘81’	‘01’	‘08’	Tipo de característica biométrica “huella digital”
					‘82’	‘01’	‘0A’	Subtipo de característica biométrica “índice izquierdo”
					‘87’	‘02’	‘01 01’	Propietario de formato JTC 1 SC 37
					‘88’	‘02’	‘00 07’	Tipo de formato [ISO/IEC 19794-4]
					Obsérvese que la BHT puede contener elementos opcionales adicionales. Por supuesto, esta huella digital puede ser de un dedo izquierdo o derecho dependiendo de la imagen disponible.			
				‘5F 2E’	Var	Datos biométricos. El bloque de datos biométricos DEBE contener exactamente una imagen de huella digital.		

Nota.— ISO/IEC 39794 sustituirá a ISO/IEC 19794:2005 como norma internacional para la codificación biométrica. Véase la sección 4.5.6.

4.7.3.2.4 Codificación de más de un caso

Para lograr la interoperabilidad, cada característica DEBE almacenarse en una plantilla de información biométrica individual. La posición de la característica DEBE especificarse dentro del subtipo de característica biométrica de CBEFF si se dispone de esa información. La tabla siguiente contiene un ejemplo elaborado para la codificación CBEFF de un elemento DG3 interoperable con dos imágenes de huellas digitales.

Tabla 52. Codificación de más de un caso

Rótulo	L	Valor				
‘63’	Var	Elemento LDS donde *aa* es la longitud total de todo el contenido de datos de LDS				
		Rótulo	**L**	**Valor**		
		‘7F 61’	Var	Plantilla de grupo de la plantilla de información biométrica.		
			‘02’	‘01’	‘02’	Define el número total de huellas digitales almacenadas como plantillas de información biométrica que siguen.

Rótulo	**L**	**Valor**						
			‘7F 60’	Var	Primera plantilla de información biométrica			
				‘A1’	Var	Plantilla de encabezamiento biométrico		
					‘81’	‘01’	‘08’	Tipo de característica biométrica “huella digital”
					‘82’	‘01’	‘0A’	Subtipo de característica biométrica “índice izquierdo”
					‘87’	‘02’	‘01 01’	Propietario de formato JTC 1 SC 37
					‘88’	‘02’	‘00 07’	Tipo de formato [ISO/IEC 19794-4]
					Obsérvese que la BHT puede contener elementos opcionales adicionales. También es posible que el orden de las huellas digitales (izquierda/derecha) sea diferente.			
				‘5F 2E’	Var	Bloque de datos biométricos. El bloque de datos biométricos DEBE contener exactamente una imagen de huella digital.		
			‘7F 60’	Var	Segunda plantilla de información biométrica			
				‘A1’	Var	Plantilla de encabezamiento biométrico		
					‘81’	‘01’	‘08’	Tipo de característica biométrica “huella digital”
					‘82’	‘01’	‘09’	Subtipo de característica biométrica “índice derecho”
					‘87’	‘02’	‘01 01’	Propietario de formato JTC 1 SC 37
					‘88’	‘02’	‘00 07’	Tipo de formato [ISO/IEC 19794-4]
					Obsérvese que la BHT puede contener elementos opcionales adicionales. También es posible que el orden de las huellas digitales (izquierda/derecha) sea diferente.			
				‘5F 2E’	Var	Bloque de datos biométricos. El bloque de datos biométricos DEBE contener exactamente una imagen de huella digital.		

Nota.— ISO/IEC 39794 sustituirá a ISO/IEC 19794:2005 como norma internacional para la codificación biométrica. Véase la sección 4.5.6.

4.7.4 GRUPO DE DATOS 4 — Elementos de identificación adicionales — Iris (OPCIONAL)

La OACI reconoce que los Estados miembros pueden optar por utilizar el reconocimiento de iris como tecnología biométrica adicional para apoyar la confirmación mecánica de la identidad, que SE CODIFICARÁ como Grupo de datos 4 (DG4).

Tabla 53. Rótulos del Grupo de datos 4

Rótulo	L	Valor
‘76’	Var	Véase codificación biométrica de EF.DG4

4.7.4.1 Codificación biométrica de EF.DG4

El DG4 DEBE utilizar la plantilla de grupo de plantillas de información biométrica (BIT) con los BITS anidados que se especifican en [ISO/IEC 7816-11], para tener la posibilidad de almacenar múltiples plantillas biométricas que se correspondan con el CBEFF. El subencabezamiento biométrico define el tipo de característica biométrica presente y la característica biométrica específica. La opción anidada de ISO/IEC [7816-11] DEBE utilizarse, incluso para codificaciones de una única plantilla biométrica. Este último caso se indica numerando con n = 1. El número de casos en el DG4 puede ser ‘0...n’.

Cada plantilla anidada tiene la estructura siguiente:

Tabla 54. Rótulos anidados del Grupo de datos 4

Rótulo	L	Valor				
‘7F61’	Var	Plantilla de grupo de la plantilla de información biométrica				
		Rótulo	**L**	**Valor**		
		‘02’	‘1’	Entero — Número de casos de este tipo de datos biométricos		
		‘7F60’	Var	Primera plantilla de información biométrica		
			Rótulo	**L**		
			‘A1’	Var	Plantilla de encabezamiento biométrico (BHT)	
				Rótulo	**L**	**Valor**
				‘80’	‘02’	Versión ‘0101’del encabezamiento de la OACI (opcional) — Versión del formato de encabezamiento patrón CBEFF
				‘81’	‘01-03’	Tipo de característica biométrica (opcional)
				‘82’	‘01’	Subtipo de característica biométrica, EXIGIDO para DG4
				‘83’	‘07’	Fecha y hora de creación (opcional)

Rótulo	**L**	**Valor**				
				‘85’	‘08’	Período de validez (desde-hasta) (opcional)
				‘86’	‘04’	Creador del dato de referencia biométrica (PID) (opcional)
				‘87’	‘02’	Propietario de formato (EXIGIDO)
				‘88’	‘02’	Tipo de formato (EXIGIDO)
			‘5F2E’ o ‘7F2E’	Var	Los datos biométricos (codificados con arreglo al propietario del formato) también se denominan bloque de datos biométricos (BDB).	
		Rótulo	**L**			
		‘7F60’	Var	Segunda plantilla de información biométrica		
			Rótulo	**L**		
			‘A1’	Var	Plantilla de encabezamiento biométrico (BHT)	
				Rótulo	**L**	**Valor**
				‘80’	‘02’	Versión ‘0101’ del encabezamiento de la OACI (opcional) — Versión del formato de encabezamiento patrón CBEFF
				‘81’	‘01-03’	Tipo de característica biométrica (opcional)
				‘82’	‘01’	Subtipo de característica biométrica EXIGIDO para DG4
				‘83’	‘07’	Fecha y hora de creación (opcional)
				‘85’	‘08’	Período de validez (desde-hasta) (opcional)
				‘86’	‘04’	Creador del dato de referencia biométrica (PID) (opcional)
				‘87’	‘02’	Propietario de formato (EXIGIDO)
				‘88’	‘02’	Tipo de formato (EXIGIDO)
			‘5F2E’ o ‘7F2E’	Var	Los datos biométricos (codificados con arreglo al propietario de formato) también se denominan bloques de datos biométricos (BDB).	

Se utiliza el OID de CBEFF por defecto. El objeto de datos OID (Rótulo ‘06’) en la plantilla de información biométrica (BIT, rótulo ‘7F60’) especificado en [ISO/IEC 7816-11] no se incluye en esta estructura. Análogamente, la autoridad de asignación de rótulo no se especifica en la estructura.

Para facilitar la interoperabilidad, la primera característica biométrica registrada en cada grupo de datos SE CODIFICARÁ con arreglo a [ISO/IEC19794-5].

Nota.— ISO/IEC 39794 sustituirá a ISO/IEC 19794:2005 como norma internacional para la codificación biométrica. Véase la sección 4.5.6.

4.7.4.2 GRUPO DE DATOS 4 — Datos EF.DG4

En esta sección se describen los datos que pueden estar presentes en el Grupo de datos 4 (DG4). Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 55. Elementos de datos para DG4

Elemento de datos	Opcional u OBLIGATORIO	Nombre del elemento de datos	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M, si se incluye característica de ojos codificada	Número de codificaciones biométricas del ojo registradas	1	F	N	1 a 9 identificando número de codificaciones únicas de datos de ojos.
02	M, si se incluye característica de ojos codificada	Encabezamiento		Var	B	El elemento de datos puede repetirse, según lo definido por el elemento de datos 01.
03	M, si se incluye característica de ojos codificada	Codificaciones biométricas de datos de ojo		Var	B	El elemento de datos puede repetirse, según lo definido por el elemento de datos 01.

4.7.4.2.1 Codificación del subtipo de datos biométricos

Los rótulos de la plantilla de encabezamiento biométrico y sus valores asignados son los mínimos que cada implementación ADMITIRÁ, como se indica en la tabla siguiente. Cada plantilla de información biométrica individual tiene la estructura siguiente:

Tabla 56. Plan para la codificación de subcaracterísticas: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Subtipo de datos biométricos
0	0	0	0	0	0	0	0	Sin información
						0	1	Derecho
						1	0	Izquierdo
			0	0	0			Reservado para uso futuro
			0	0	1			Reservado para uso futuro
			0	1	0			Reservado para uso futuro

b8	b7	b6	b5	b4	b3	b2	b1	Subtipo de datos biométricos
			0	1	1			Reservado para uso futuro
			1	0	0			Reservado para uso futuro
			1	0	1			Reservado para uso futuro
X	X	X						Reservado para uso futuro

4.7.4.2.2 Codificación de cero casos

Los Estados que no expiden LDS1 de eMRTD con datos de iris NO DEBERÍAN rellenar el DG4. El DG4 de esta estructura presenta el inconveniente de que resultará en una condensación estática del DG4 en el SO_D para todas las LDS1 de eMRTD donde los datos biométricos no están presentes y no se rellenan en el momento de expedición de la LDS1 del eMRTD pero se ha declarado el DG4. Para fines de interoperabilidad, los Estados que apoyan el reconocimiento de iris en sus LDS1 del eMRTD DEBEN almacenar una plantilla del grupo de información biométrica vacía en los casos en que no se disponga de datos de iris en el momento de expedición de la LDS! del eMRTD. En este caso, el contador de la plantilla indica un valor de '00'.

Se RECOMIENDA añadir el rótulo '53' con contenido definido por el expedidor (p. ej., un número aleatorio).

Tabla 57. Codificación de cero casos

<table>
<tr><th>Rótulo</th><th>L</th><th colspan="5">Valor</th></tr>
<tr><td>'76'</td><td>Var</td><td colspan="5">Elemento LDS</td></tr>
<tr><td></td><td></td><td>Rótulo</td><td>L</td><td colspan="3">Valor</td></tr>
<tr><td></td><td></td><td>'7F 61'</td><td>'03'</td><td colspan="3">Plantilla de grupo de la plantilla de información biométrica</td></tr>
<tr><td></td><td></td><td></td><td>'02'</td><td>'01'</td><td>'00'</td><td>Define que en este grupo de datos no hay plantillas de información biométrica almacenadas.</td></tr>
<tr><td></td><td></td><td>'53'</td><td>Var</td><td colspan="3">Contenido definido por el expedidor (p. ej., un número aleatorio).</td></tr>
</table>

4.7.4.2.3 Codificación de un caso

En los casos en que solo se dispone de un iris, DEBE codificarse el caso único.

4.7.4.2.4 Codificación de más de un caso

Para lograr la interoperabilidad, cada característica DEBE almacenarse en una plantilla de información biométrica individual. La posición de la característica DEBE especificarse dentro del subtipo de característica biométrica CBEFF si se dispone de esa información.

4.7.5 GRUPO DE DATOS 5 — Retrato exhibido (OPCIONAL)

Los elementos de datos asignados al grupo de datos 5 (DG5) SERÁN los siguientes:

Tabla 58. Rótulos del grupo de datos 5

Rótulo	L	Valor		
'65'	Var			
		Rótulo	**L**	**Valor**
		'02'	Var	Número de casos de este tipo de imagen exhibida (EXIGIDO en la primera plantilla. No se utiliza en plantillas subsiguientes).
		'5F40'	Var	Retrato exhibido

Se reconocen los siguientes propietarios de formato para el tipo de imagen exhibida especificado.

Tabla 59. Formatos DG5

Imagen exhibida	Propietario de formato
Imagen facial exhibida	[ISO/IEC 10918], opción JFIF

4.7.5.1 GRUPO DE DATOS 5 — Datos de EF.DG5 (Opcional)

En esta sección se describen los datos que pueden estar presentes en el Grupo de datos 5 (DG5). Los datos y su formato dentro del DG5 SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 60. Elementos de datos para DG5

Dato	Opcional u OBLIGATORIO	Nombre del elemento de datos	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M (si se incluye el retrato exhibido)	Número de retratos exhibidos registrados	1	F	N	1 a 9 identificando número de registros únicos de retrato exhibido.
02	M (si se incluye el retrato exhibido)	Representación del retrato exhibido		Var	A, N	El elemento de datos puede repetirse, según lo definido por el elemento de datos 01.

Dato	Opcional u OBLIGATORIO	Nombre del elemento de datos	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
03	M (si se incluye el retrato exhibido)	Número de bytes en representación del retrato exhibido	5	F	N	00001 a X9, identificando el número de bytes en representación de retrato exhibido que sigue inmediatamente.
04	M (si se incluye el retrato exhibido)	Representación del retrato exhibido		Var	B	Formateado según [ISO/IEC 10918-1] o [ISO/IEC 15444].

Nota.— El dato 02 se REGISTRARÁ como se define en [ISO/IEC 10918], utilizando la opción JFIF o la [ISO/IEC 15444] utilizando el sistema de codificación de imágenes JPEG 2000.

4.7.6 GRUPO DE DATOS 6 — Reservado para uso futuro

Los elementos de datos asignados al grupo de datos 6 (DG6) SERÁN los siguientes:

Tabla 61. Rótulos del Grupo de datos 6

Rótulo	L	Valor
‘66’	Var	

4.7.6.1 GRUPO DE DATOS 6 — Elementos de datos de EF.DG6

Los elementos de datos para el DG6 se reservan para uso futuro.

4.7.7 GRUPO DE DATOS 7 — Firma o marca habitual exhibida (OPCIONAL)

Los elementos de datos asignados al grupo de datos 7 (DG7) SERÁN los siguientes:

Tabla 62. Rótulos del Grupo de datos 7

Rótulo	L	Valor		
‘67’	Var			
		Rótulo	**L**	**Valor**
		‘02’	Var	Número de casos de este tipo de imagen exhibida (EXIGIDO en la primera plantilla. No se utilizan las plantillas subsiguientes).
		‘5F43’	Var	Firma exhibida.

Se reconocen los siguientes propietarios de formatos para el tipo de imagen exhibida especificado:

Tabla 63. Formatos de DG7

Imagen exhibida	Propietario de formato
Firma/marca habitual exhibida	[ISO/IEC 10918], opción JFIF

4.7.7.1 GRUPO DE DATOS 7 — Datos de EF.DG7 (OPCIONAL)

En esta sección se describen los datos que pueden estar presentes en el Grupo de datos 7 (DG7). Los datos y su formato dentro del DG7 SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 64. Elementos de datos para DG7

Dato	Opcional u OBLIGATORIO	Nombre del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M (Si se incluye firma o marca habitual exhibida)	Número de firmas o marcas habituales exhibidas	1	F	N	1 a 9 identificando el número de registros únicos de firma o marca habitual exhibidas.
02	M (Si se incluye firma o marca habitual exhibida)	Representación de firma o marca habitual exhibidas		Var	B	El dato puede repetirse según lo definido por DE 01. Formateado según [ISO/IEC 10918-1] o [ISO/IEC 15444].

Nota.— El dato 02 SE CODIFICARÁ según se define en [ISO/IEC 10918], utilizando la opción JFIF, o en [ISO/IEC 15444] utilizando el sistema de codificación de imágenes JPEG 2000.

4.7.8 GRUPO DE DATOS 8 — Elemento datos (OPCIONAL)

Este grupo de datos no se ha definido aún. Hasta entonces, los datos están disponibles para uso patentado temporario. Estos datos podrían utilizar una estructura similar a la de plantillas biométricas, verificación mecánica de elementos de seguridad y detalles codificados. Los datos que se combinan para formar el Grupo de datos 8 (DG8) SERÁN los siguientes:

Tabla 65. Rótulos del Grupo de datos 8

Rótulo	L	Valor		
'68'	Var	Por definir		
		Rótulo	**L**	**Valor**
		'02'	'1'	Entero — Número de casos de este tipo de plantilla (EXIGIDO en la primera plantilla. No se utiliza en las plantillas subsiguientes).
			Var	Plantilla de encabezamiento. Detalles por definir.

4.7.8.1 GRUPO DE DATOS 8 — Datos del EF.DG8

En esta sección se describen los datos que pueden estar presentes en el DG8. Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 66. Elementos de datos para DG8

Dato	Opcional u OBLIGATORIO	Nombre del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M (Si se incluye este elemento codificado)	Número de elementos datos	1	F	N	1 a 9, identificando número de codificaciones únicas de elementos datos (abarca del elemento de datos 02 al 03).
02	M (Si se incluye este elemento codificado)	Encabezamiento (por definir)	1			Se definirán detalles de encabezamiento.
03	M (Si se incluye este elemento codificado)	Datos del elemento datos	999 Máx	Var	A, N, S, U, B	Formato definido a discreción del Estado expedidor u organización expedidora.

4.7.9 GRUPO DE DATOS 9 — Elemento estructura (OPCIONAL)

Este grupo de datos no se ha definido aún. Hasta entonces, los datos están disponibles para uso patentado temporario. Estos datos podrían utilizar una estructura similar a la de plantilla biométrica. Los datos que se combinan para formar el Grupo de datos 9 (DG9) SERÁN los siguientes:

Tabla 67 Rótulos del Grupo de datos 9

Rótulo	L	Valor		
‘69’	Var	Por definir		
		Rótulo	**L**	**Valor**
		‘02’	‘01’	Entero — Número de casos de este tipo de plantilla (EXIGIDO en la primera plantilla. No se utiliza en las plantillas subsiguientes).
			X	Plantilla de encabezamiento. Se definirán los detalles.

4.7.9.1 GRUPO DE DATOS 9 — Datos de EF.DG9

Los elementos de datos del DG9 y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial [‘<’], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 68. Datos para DG9

Dato	Opcional u OBLIGATORIO	Nombre del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M (Si se incluye este elemento codificado)	Número de elementos de estructura	1	F	N	1 a 9, identificando el número de codificaciones únicas de elementos estructura (abarca del elemento de datos 02 al 03).
02	M (Si se incluye este elemento codificado)	Encabezamiento (por definir)			N	Se definirán detalles de encabezamiento.
03	M (Si se incluye este elemento codificado)	Datos del elemento estructura		Var	B	

4.7.10 GRUPO DE DATOS 10 — Elemento substancia (OPCIONAL)

Este grupo de datos no se ha definido aún. Hasta entonces, los datos están disponibles para uso patentado temporario. Estos datos podrían utilizar una estructura similar a la de las plantillas biométricas. Los datos que se combinan para formar el Grupo de datos 10 (DG10) SERÁN los siguientes:

Tabla 69. Rótulos de Grupo de datos 10

Rótulo	L	Valor		
'6A'	Var			
		Rótulo	**L**	**Valor**
		'02'	'01'	Entero — Número de casos de este tipo de plantilla (EXIGIDO en la primera plantilla. No se utiliza en plantillas subsiguientes).
			Var	Por definir.

4.7.10.1 GRUPO DE DATOS 10 — Datos de EF.DG10

En esta sección se describen los datos que pueden estar presentes en el DG10. Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 70. Elementos de datos para DG10

Dato	Opcional u OBLIGATORIO	Nombre del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M (Si se incluye este elemento codificado)	Número de elementos substancia registrados	1	F	N	1 a 9, identificando un número de codificaciones únicas de elementos substancia (abarca del elemento de datos 02 al 03).
02	M (Si se incluye este elemento codificado)	Encabezamiento (por definir)	TBD	TBD	N	Se definirán detalles.
03	M (Si se incluye este elemento codificado)	Datos del elemento substancia	999 Máx	Var	A, N, S, U, B	Formato definido a discreción del Estado expedidor u organización expedidora.

4.7.11 GRUPO DE DATOS 11 — Detalles personales adicionales (OPCIONAL)

Este grupo de datos se utiliza para detalles adicionales respecto al titular del documento. Dado que todos los datos del grupo son opcionales, se utiliza una lista de rótulos para definir los que están presentes. Los datos que se combinan para formar el Grupo de datos 11 (DG11) SERÁN los siguientes:

Nota.— Esta plantilla puede contener caracteres no latinos.

Tabla 71. Rótulos del Grupo de datos 11

Rótulo	**L**	**Valor**				
‘6B’	Var					
		Rótulo	**L**	**Valor**		
		‘5C’	Var			Lista de rótulos con lista de elementos de datos en la plantilla.
		‘5F0E’	Var			Nombre completo del titular del documento en caracteres nacionales. Codificados según reglas del Doc 9303.
		‘A0’	Var			Clase construida con arreglo al contenido
				Rótulo	**L**	**Valor**
				‘02’	‘01’	Número de otros nombres
				‘5F0F’	Var	Otro nombre formateado según Doc 9303. El objeto de datos se repite tantas veces como se especifica en el número de otros nombres (objeto de datos con rótulo ‘02’)
		Rótulo	**L**	**Valor**		
		‘5F10’	Var			Número personal
		‘5F2B’	08			Fecha de nacimiento completa aaaammdd
		‘5F11’	Var			Lugar de nacimiento. Campos separados por ‘<’
		‘5F42’	Var			Dirección permanente. Campos separados por ‘<’
		‘5F12’	Var			Teléfono
		‘5F13’	Var			Profesión
		‘5F14’	Var			Título
		‘5F15’	Var			Resumen personal
		‘5F16’	Var			Prueba de ciudadanía. Imagen comprimida según [ISO/IEC 10918]
		‘5F17’	Var			Otros números de documentos de viaje válidos TD. Separados por ‘<’
		‘5F18	Var			Información de custodia

4.7.11.1 GRUPO DE DATOS 11 — Datos de EF.DG11

En esta sección se describen los datos que pueden estar presentes en el DG11. Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota 1.— El DG11 se CODIFICARÁ según se define en [ISO/IEC 10918], utilizando la opción JFIF o en la [ISO/IEC 15444] utilizando el sistema de codificación de imágenes JPEG 2000.

Nota 2.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial [‘<’], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 72. Datos para DG11

Dato	Opcional u OBLIGATORIO	Nombre del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	O	Nombre del titular (completo)	99 Máx	Var	B	Caracteres de relleno (<) insertados para ZLM. No se insertan caracteres de relleno al final de la línea. No se permite truncamiento.
02	O	Otros nombres	99 Máx	Var	B	Caracteres de relleno (<) insertados para ZLM. No se insertan caracteres de relleno al final de la línea. No se permite truncamiento.
03	O	Número personal	99 Máx	Var	U	Texto libre.
04	O	Fecha de nacimiento completa	8	F	N	AAAAMMDD
05	O	Lugar de nacimiento	99 Máx	Var	U	Texto libre.
06	O	Dirección	99 Máx	Var	U	Texto libre.
07	O	Teléfono	99 Máx	Var	N, S	Texto libre. Se recomienda la codificación con arreglo a ITU-T E.164.
08	O	Profesión	99 Máx	Var	U	Texto libre.
09	M, si se incluye el elemento de dato 08	Título	99 Máx	Var	U	Texto libre.
10	M, si se incluye el elemento de dato 09	Resumen personal	99 Máx	Var	U	Texto libre.
11	M, si se incluye el elemento de dato 10	Prueba de ciudadanía		Var	B	Imagen del documento de ciudadanía formateado según [ISO/IEC 10918-1]
12	O	Otros documentos de viaje válidos Número de documento de viaje	99 Máx	Var	U	Texto libre, separado por <.
13	O	Información de custodia	999 Máx	Var	U	Texto libre.

Nota.— Si se desconoce el mes (MM) o el día (DD), la manera interfuncional de indicarlo en DG11 es poner los caracteres respectivos a '00'. Si se desconoce el siglo y el año (SSAA), la manera interfuncional de indicarlo en DG11 es poner los caracteres respectivos a '0000'. Las fechas asignadas por el expedidor DEBEN siempre utilizarse en forma coherente.

4.7.12 GRUPO DE DATOS 12 — Detalles del documento adicionales (OPCIONAL)

Este grupo de datos se utiliza para información adicional sobre el documento. Todos los datos de este grupo son opcionales.

Tabla 73. Rótulos del Grupo de datos 12

Rótulo	**L**	**Valor**				
'6C'	Var					
		Rótulo	**L**	**Valor**		
		'5C'	Var			Lista de rótulos con lista de elementos de datos en la plantilla
		'5F19'	Var			Autoridad expedidora
		'5F26'	08			Fecha de expedición. aaaammdd
		'A0'	Var			Construido con arreglo al contenido específico
				Rótulo	**L**	**Valor**
				'02'	'01'	Número de otras personas
				'5F1A'	Var	Nombre de otra persona formateado según las reglas del Doc 9303. El objeto de datos se repite tantas veces como se indique en el número de otros nombres del elemento de datos 02 (objeto de datos con rótulo '02').
		Rótulo	**L**	**Valor**		
		'5F1B'	Var			Aprobaciones, observaciones
		'5F1C'	Var			Requisitos impositivos/de salida
		'5F1D'	Var			Imagen anterior del documento. Según ISO/IEC 10918
		'5F1E'	Var			Imagen posterior del documento. Según ISO/IEC 10918
		'5F55'	0E			Fecha y hora de personalización del documento aaaammddhhmmss
		'5F56'	Var			Número de serie del sistema de personalización

Se RECOMIENDA que los sistemas de inspección apoyen la codificación ASCII de 8 bytes y la BCD de fecha/hora.

4.7.12.1 GRUPO DE DATOS 12 — Datos de EF.DG12

En esta sección se describen los datos que pueden estar presentes en el Grupo de datos 12 (DG12). Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota 1.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Nota 2.— Los datos 07 y 08 SE CODIFICARÁN según se define en [ISO/IEC 10918], utilizando la opción JFIF o en la [ISO/IEC 15444] utilizando el sistema de codificación de imágenes JPEG 2000.

Tabla 74. Datos para DG12

Dato	Opcional u OBLIGATORIO	Nombre del elemento de dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	O	Autoridad expedidora	99 Máx	Var	U	Texto libre.
02	O	Fecha de expedición	8	F	N	Fecha de expedición del documento; AAAAMMDD.
03	O	Detalles de otras personas	99 Máx	Var	U	Texto libre
04	O	Aprobaciones/ observaciones	99 Máx	Var	U	Texto libre.
05	O	Requisitos impositivos/de salida	99 Máx	Var	U	Texto libre.
06	O	Imagen del anverso del eMRTD		Var	B	Formateada según [ISO/IEC 10918-1]
07	O	Imagen del reverso del MRTD		Var	B	Formateada según [ISO/IEC 10918-1]
08	O	Hora de personalización	14	F	N	aaaammddhhmmss
09	O	Número de serie de dispositivo de personalización	99 Máx	Var	U	Formato libre.

4.7.13 GRUPO DE DATOS 13 — Detalles opcionales (OPCIONAL)

Los datos que se combinan para formar el Grupo de datos 13 (DG13) quedan a discreción del Estado expedidor u organización expedidora y SERÁN los siguientes:

Tabla 75. Rótulos del Grupo de datos 13

Rótulo	L	Valor
'6D'	Var	

4.7.14 GRUPO DE DATOS 14 — Opciones de seguridad (CONDICIONAL)

El grupo de datos 14 (DG14) contiene opciones de seguridad para mecanismos de seguridad adicionales. Para más detalles véase el Doc 9303-11. El fichero DG14 contenido en la aplicación del eMRTD se EXIGE si la autenticación de la microplaqueta o PACE-GM/-IM es admitido por la microplaqueta del eMRTD.

Tabla 76. Rótulos del gupo de datos 14

Rótulo	L	Valor
'6E	Var	Véase el DG14 SecurityInfos del Doc 9303-10

4.7.14.1 GRUPO DE DATOS 14 — Datos de EF.DG14

En esta sección se describen los datos que pueden estar presentes en el DG14. Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota 1.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 77. Elementos de datos para DG14

Dato	Opcional u OBLIGATORIO	Nombre del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
	O	SecurityInfos		Var	B	Véase el Doc 9303-10. Los SecurityInfos del DG14 se definen en 4.7.14.2

4.7.14.2 GRUPO DE DATOS 14 — Datos de SecurityInfos

Los siguientes datos SecurityInfos de la estructura genérica de datos ASN.1 permiten varias formas de implantación de opciones de seguridad para datos biométricos secundarios. Por razones de interfuncionamiento, se RECOMIENDA que esta estructura de datos se proporcione por la microplaqueta eMRTD en el DG14 para indicar los protocolos de seguridad apoyados. La estructura de datos se especifica como sigue:

```
      SecurityInfos     ::=   SET of SecurityInfo

      SecurityInfo      ::=   SEQUENCE {
            protocol          OBJECT IDENTIFIER,
            requiredData      ANY DEFINED BY protocol,
            optionalData      ANY DEFINED BY protocol OPTIONAL
}
```

Los elementos contenidos en una estructura de datos SecurityInfo tienen el significado siguiente:

- El protocolo identificador de objeto identifica al protocolo apoyado;
- El elemento requiredData de tipo abierto contiene datos obligatorios específicos del protocolo;
- El elemento optionalData de tipo abierto contiene datos opcionales específicos del protocolo.

4.7.15 GRUPO DE DATOS 15 — Información de clave pública de autenticación activa (CONDICIONAL)

Este Grupo de datos OPCIONAL contiene la clave pública de autenticación active y se EXIGE cuando se implanta la autenticación opcional de microplaqueta de autenticación activa como se describe en el Doc 9303-11.

Tabla 78. Rótulos del Grupo de datos 15

Rótulo	L	Valor
‘6F	Var	Véase el Doc 9303-11

4.7.15.1 *GRUPO DE DATOS 15 — Datos de EF.DG15*

En esta sección se describen los datos que pueden estar presentes en el Grupo de datos 15 (DG15). Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota 1.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial [‘<’], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 79. Datos para DG15

Dato	Opcional u OBLIGATORIO	Nombre del elemento de dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
	O	ActiveAuthenti-cationPublicKey Info		Var	B	Véase el Doc 9303-11

4.7.16 GRUPO DE DATOS 16 — Personas que han de notificarse (OPCIONAL)

Este grupo de datos contiene información de notificación de emergencia. Está codificado como serie de plantillas con la designación de Rótulo 'Ax'. El grupo de datos 16 (DG16) (como todos los otros grupos de datos) no DEBERÍA actualizarse después de la expedición; el DG16 se representa mediante un valor de condensación en el SO_D y el SO_D solo se firma una vez en la expedición.

Tabla 80. Rótulos del Grupo de datos 16

Rótulo	L	Valor		
'70'	Var			
		Rótulo	**L**	**Valor**
		'02'	'01'	Número de plantillas (solo en la primera plantilla)
		'Ax'	Var	Inicio de la plantilla, donde x (x=1,2,3…) aumenta con cada ocurrencia
'5F50'	'08'			Fecha de registro de datos
'5F51'	Var			Nombre de la persona
'5F52'	Var			Teléfono
'5F53'	Var			Dirección

4.7.16.1 GRUPO DE DATOS 16 — Elementos de datos de EF.DG16

En esta sección se describen los datos que pueden estar presentes en el DG16. Los datos y su formato dentro del grupo de datos SERÁN los que se indican en la tabla siguiente:

Nota 1.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial ['<'], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Tabla 81. Datos para DG16

Dato	Opcional u OBLIGATORIO	Nombre del elemento del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
01	M, si se incluye DG16	Número de personas identificadas	1	F	N	Identifica el número de personas incluidas en el grupo de datos.
02	M, si se incluye DG16	Detalle de fecha registrado	8	F	N	Fecha de registro de la fecha de notificación; formato = AAAAMMDD.

Dato	Opcional u OBLIGATORIO	Nombre del elemento del dato	Núm. de bytes	Fijo o variable	Tipo de codificación	Requisitos de codificación
03	M, si se incluye DG16	Número de personas a notificar. Identificadores primarios y secundarios		Var	A, N, S	Caracteres de relleno (<) insertados como en la ZLM. No se permite truncamiento.
04	M, si se incluye el elemento de dato 03	Número telefónico de la persona que ha de notificarse		Var	N, S	Número telefónico en forma internacional (código de país y número local). Se recomienda la codificación con arreglo a ITU-T E.164.
05	M	Dirección de la persona que ha de notificarse		Var	U	Texto libre.

5. APLICACIONES DE LA LDS2 (OPCIONAL)

La estructura lógica de datos 2 (LDS2) es una extensión retrocompatible y opcional de la LDS1 para la microplaqueta de eMRTD que permitiría el almacenamiento digital y seguro de la información de viaje después de la expedición del documento. La LDS2 amplía el uso del eMRTD añadiendo aplicaciones que podrían permitir el almacenamiento digital de los datos de viaje (visados y sellos de viaje) y otra información que podría facilitar el viaje de la persona titular (datos biométricos adicionales) durante su período de validez. El mejor aprovechamiento del potencial pleno del eMRTD gracias a la "digitalización" del resto de los datos contenidos en los documentos ofrece una serie de beneficios de facilitación, a la vez que aumenta la protección del documento para evitar que sea objeto de falsificación, copia o lectura y escritura no autorizadas.

Las aplicaciones adicionales y opcionales descritas como LDS2 son las siguientes:

- registros de viaje (sellos);
- visados electrónicos; y
- datos biométricos adicionales.

Es OBLIGATORIO que la aplicación de la LDS1 del eMRTD esté presente antes de que se declare ninguna aplicación de la LDS2 OPCIONAL.

5.1 Aplicación de registros de viaje (CONDICIONAL)

La aplicación de registros de viaje PUEDE ser implementada por un Estado expedidor o una organización expedidora. Si se ha invocado la aplicación de los registros de viaje opcional, SE EXIGE de forma condicional lo siguiente:

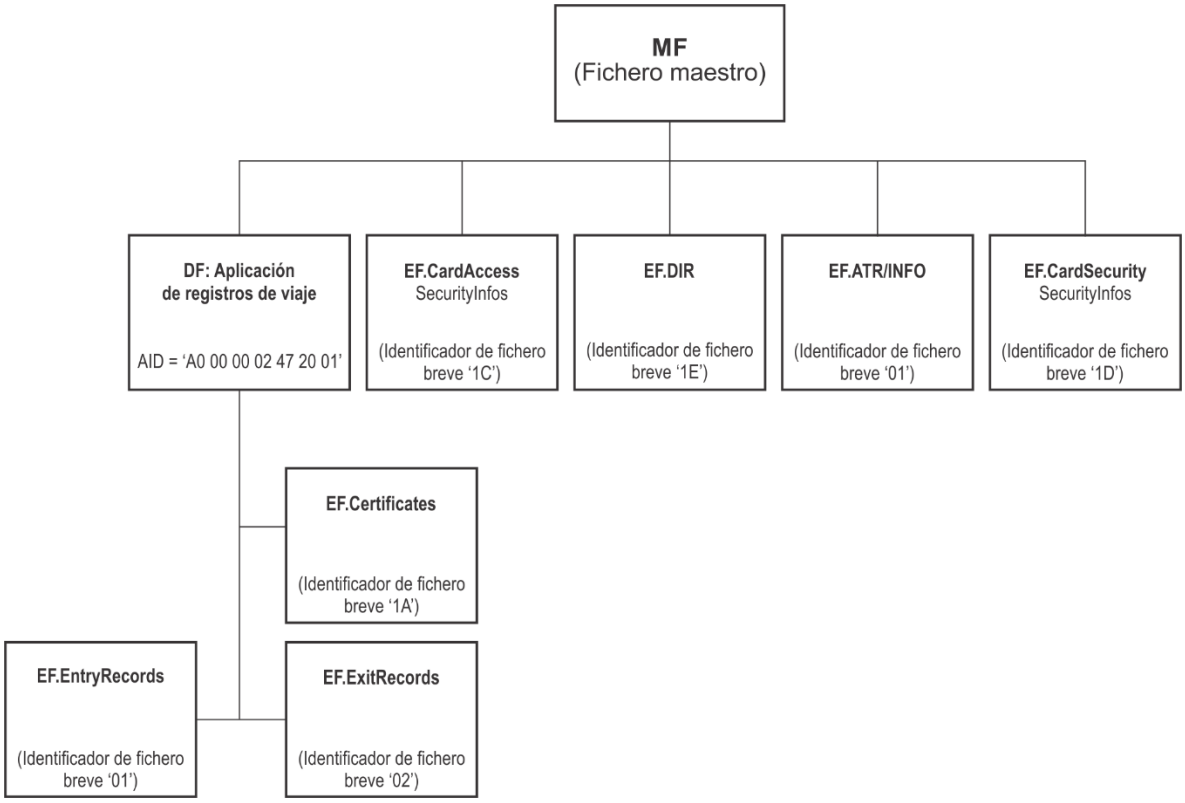


Figura 4. Estructura de los registros de viaje

Los registros de los viajes de entrada y salida se almacenan en dos ficheros elementales separados, EF.EntryRecords y EF.ExitRecords, en el DF para la aplicación de los registros de viaje, teniendo ambos una estructura lineal con registros de tamaño variable, con arreglo a [ISO/IEC 7816-4]. Los certificados de firmante del registro de viaje se almacenan en un fichero elemental separado EF.Certificates, que tiene una estructura lineal con registros de tamaño variable.

5.1.1 Selección de aplicación — DF

La aplicación de registros de viaje DEBE seleccionarse utilizando el identificador de la aplicación (AID) como nombre DF reservado. El AID DEBE constar del identificador de la aplicación registrado asignado por la ISO con arreglo a [ISO/IEC 7816-5], seguido por la extensión de identificador de aplicación de propiedad (PIX) de la aplicación de los registros de viaje:

- el identificador de la aplicación registrado es 'A0 00 00 02 47';
- la aplicación de los registros de viaje DEBE usar PIX = '20 01'; y
- el AID completo de la aplicación de los registros de viaje DEBE ser 'A0 00 00 02 47 20 01'.

El CI DEBE rechazar la selección de esta aplicación si la autorización efectiva no garantiza derechos de acceso a ningún dato de una aplicación de la LDS2.

5.1.2 EF.Certificates (OBLIGATORIO)

Los certificados de firmante del registro de viaje se almacenan en un EF dentro del DF de la aplicación y tienen una estructura lineal con registros de tamaño variable. Está previsto que el IS utilice estos certificados para realizar una nueva validación fuera de línea de las firmas digitales para cada registro tanto en el fichero EF.ExitRecords como en el EF.EntryRecords files.

Tabla 82. EF.Certificates

Nombre del fichero	EF.Certificates
ID del fichero	‘011A’
Identificador EF breve	‘1A’
Seleccionar / Access FMM	PACE+TA (Bit b3 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Read record / Search Record (leer/buscar registro)	PACE+TA (Bit b3 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Append Record (añadir registro)	PACE+TA (Bit b4 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Write / Update Record (escribir/actualizar registro)	NUNCA
Acceso a Erase Record (borrar registro)	NUNCA
Estructura del fichero	Estructura lineal con registros de tamaño variable
Tamaño	Variable

El registro del certificado contiene un un solo objeto de datos del certificado X.509 del firmante de la LDS2-V. Un registro de certificado PUEDE constar como referencia en uno o más registros de viaje de entrada o salida.

Tabla 83. Formato del registro EF.Certificates

Rótulo	Contenido	Obligatorio /Opcional	Formato	Ejemplo
‘5F3A’	Número de serie del certificado	M	V(22)B	‘5F3A’ ‘Len’ {Código de país || Número de serie }
‘72’	Certificado X.509	M	V (900) B	‘72’ ‘Len’ { Certificado X.509 }

Nota.— Los rótulos interindustriales especificados en esta tabla se usan en el contexto de la LDS, así que no es necesario un sistema de asignación de rótulos coexistentes.

El DO’5F3A’ DEBE contener un código de país de dos letras, conforme al Doc 9303, Parte 3 (misma codificación y valor que el countryName (nombre del país) que expide el X.509 en el certificado del sujeto, seguido por el número de serie del certificado.

Cada certificado X.509 contiene un conjunto de elementos de datos codificados en ASN.1 ilustrados en la tabla 84. En la especificación de perfiles de certificado del Doc 9303-12 pueden encontrarse los requisitos detallados para el certificado X.509.

Tabla 84. Ejemplo de estructura del certificado X.509

Campo			Descripción	Valor del ejemplo
Certificado				
	version		Debe ser la versión 3	2
	serialNumber		Número entero positivo único	20 bytes máx.
	firma		Algoritmo de firma	ecdsa-with-SHA256
	expedidor			
		countryName	Nombre del país expedidor	‘EE. UU.’
		commonName	Nombre del expedidor (9 caracteres máx.)	‘DHSCA0001’
	validez			
		notBefore	Fecha efectiva del cert.	‘131225000000Z’
		notAfter	Fecha de caducidad del cert.	‘230824235959Z’
	subject			
		countryName	Nombre del país del IS	‘EE. UU.’
		commonName	Nombre del IS (9 caracteres máx.)	‘SFO000001’
	subjectPublicKeyInfo			
		Algoritmo de clave pública	ecPublicKey	
		Clave pública de asunto	Clave pública del IS	Clave pública ECC256
	extensiones			
		AuthorityKeyIdentifier		
		ExtKeyUsage		
Algoritmo de firma			ecdsa-with-SHA256	
Firma			Firma del expedidor	Firma ECDSA256

Nota.— Esta tabla es un ejemplo que se presenta solo a título ilustrativo. Los registros de certificado se escriben en EF.Certificates, ubicado en el DF de la aplicación de los registros de viaje, usando el comando APPEND RECORD. Los registros de certificado pueden leerse de EF.Certificates utilizando el comando READ RECORD. Los registros de certificado NO DEBEN actualizarse ni borrarse. El número máximo de registros en EF.Certificates en el DF de la aplicación de los registros de viaje DEBE ser de 254.

5.1.3 EF.ExitRecords (OBLIGATORIO)

Los registros de salida DEBEN ser añadidos por un IS autorizado en el momento del embarque.

Tabla 85. EF.ExitRecords

Nombre del fichero	EF.ExitRecords
ID del fichero	‘0102’
Identificador EF breve	‘02 ’
Seleccionar / Access FMM	PACE+TA (Bit b1 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Read record / Search Record (leer/buscar registro)	PACE+TA (Bit b1 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Append Record (añadir registro)	PACE+TA (Bit b2 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Write / Update Record (escribir/actualizar registro)	NUNCA
Acceso a Erase Record (borrar registro)	NUNCA
Estructura del fichero	Estructura lineal con registros de tamaño variable
Tamaño	Variable

En la tabla 86 se muestra el contenido de un registro de salida.

Nota.— Los rótulos interindustriales especificados en la tabla siguiente se usan en el contexto de la LDS, así que no es necesario un sistema de asignación de rótulos coexistentes.

Tabla 86. Formato de registro de entrada/salida

Rótulo	Rótulo	Contenido	Obligatorio /OPCIONAL	Formato	Ejemplo
‘5F44’		Estado de embarque/desembarque (copia para SEARCH RECORD)	M	F (3) A	Estados Unidos
‘73’	Registro de entrada/salida (información firmada)				
	‘5F44’	Estado de embarque/desembarque	M	F (3) A	Estados Unidos
	‘5F4C’	Aprobación, denegación y retirada de visado	O	V (50) A, N, S, U	Texto libre
	‘5F45’	Fecha de viaje (fecha de entrada/salida)	M	F (8) N	20120814 (aaaammdd)
	‘5F4B’	Autoridad de inspección	M	V (10) A, N, S	CBP

Rótulo	Rótulo	Contenido	Obligatorio /OPCIONAL	Formato	Ejemplo
	‘5F46’	Lugar de inspección (puerto de entrada/salida)	M	V (10) A, N, S	SFO
	‘5F4A’	Referencia del inspector/a	M	V (20) A, N, S	SFO00001234
	‘5F4D’	Resultado de la inspección	O	V (50) A, N, S, U	Texto libre
	‘5F49’	Modo de viaje	O	F (1) A	A (aire), S (mar), L (tierra)
	‘5F48’	Duración de la estancia (días)	O	V (2) B	‘00FF’ (255 días)
	‘5F4E’	Condiciones que debe cumplir la persona titular mientras esté en el Estado expedidor	O	V(50) A, N, S, U	Texto libre
‘5F37’	Testigos de autenticación (firma)		M	V (140) B	‘5F’ ‘37’ Len {firma}
‘5F38’	Referencia (número de registro) al certificado del firmante de la LDS2-TS en el almacén de certificados		M	F (1) B	‘01’ …’FE’

Nota 1.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial [‘<’], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable.

Nota 2.— Dado que es probable que los certificados de firmante de la LDS2-TS sean los mismos que en múltiples registros de viaje (p. ej., cuando se entra y sale de un país por el mismo aeropuerto con un solo firmante LDS2-TS), antes de escribir/añadir un nuevo certificado a EF.Certificates, el IS debería buscar en EF.Certificates una copia del mismo certificado y referenciar el existente. Esto reducirá el tamaño de EF.Certificates y hará posible que se hagan búsquedas más rápidas.

Nota 3.— La LDS2 del eMRTD no impone que un IS escriba los Entry Records solo en los EF.EntryRecords y no en los EF.ExitRecords, y viceversa.

Nota 4.— Código de tres letras del estado de embarque/desembarque con arreglo al Doc 9303-3.

El orden de los objetos de datos de un registro es fijo. El IS DEBE establecer el contenido del registro utilizando los objetos de datos en el orden especificado en la tabla.

Cada registro DEBE contener una firma digital (testigo de autenticación) calculada sobre el DO’73’, incluidos el rótulo 73 y la longitud. La firma es generada por el firmante de la LDS2-TS.
Los certificados de firmante de la LDS2-TS exigidos para verificar la firma del registro de viaje DEBEN almacenarse en EF.Certificates en el DF de la aplicación de los registros de viaje si todavía no está disponible en el mismo fichero.

Los registros de viaje se escriben (añaden) en el EF utilizando APPEND RECORD. Estos registros NO DEBEN alterarse (actualizarse) ni borrarse. El número máximo de registros permitidos en cada EF DEBE ser de 254.

5.1.4 EF.EntryRecords (OBLIGATORIO)

Los registros de entrada DEBEN ser añadidos por un IS autorizado en el momento del desembarque.

Tabla 87. EF.EntryRecords

Nombre del fichero	EF.EntryRecords
ID del fichero	'0101'
Identificador EF breve	'01'
Seleccionar / Acceso FMM	PACE+TA (Bit b1 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Read record / Search Record (leer/buscar registro)	PACE+TA (Bit b1 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Append Record (añadir registro)	PACE+TA (Bit b2 de la autorización del registro de viaje con arreglo a la tabla 96)
Acceso a Write / Update Record (escribir/actualizar registro)	NUNCA
Acceso a Erase Record (borrar registro)	NUNCA
Estructura del fichero	Estructura lineal con registros de tamaño variable
Tamaño	Variable

La estructura del registro de entrada es idéntica a la estructura del registro de salida que se especifica en la tabla 86.

5.2 Aplicación de los registros de visados (CONDICIONAL)

La aplicación de los registros de visados PUEDE ser implementada por un Estado expedidor o una organización expedidora. Si se ha invocado la aplicación de registros de visados opcional, SE EXIGE de forma condicional lo siguiente:

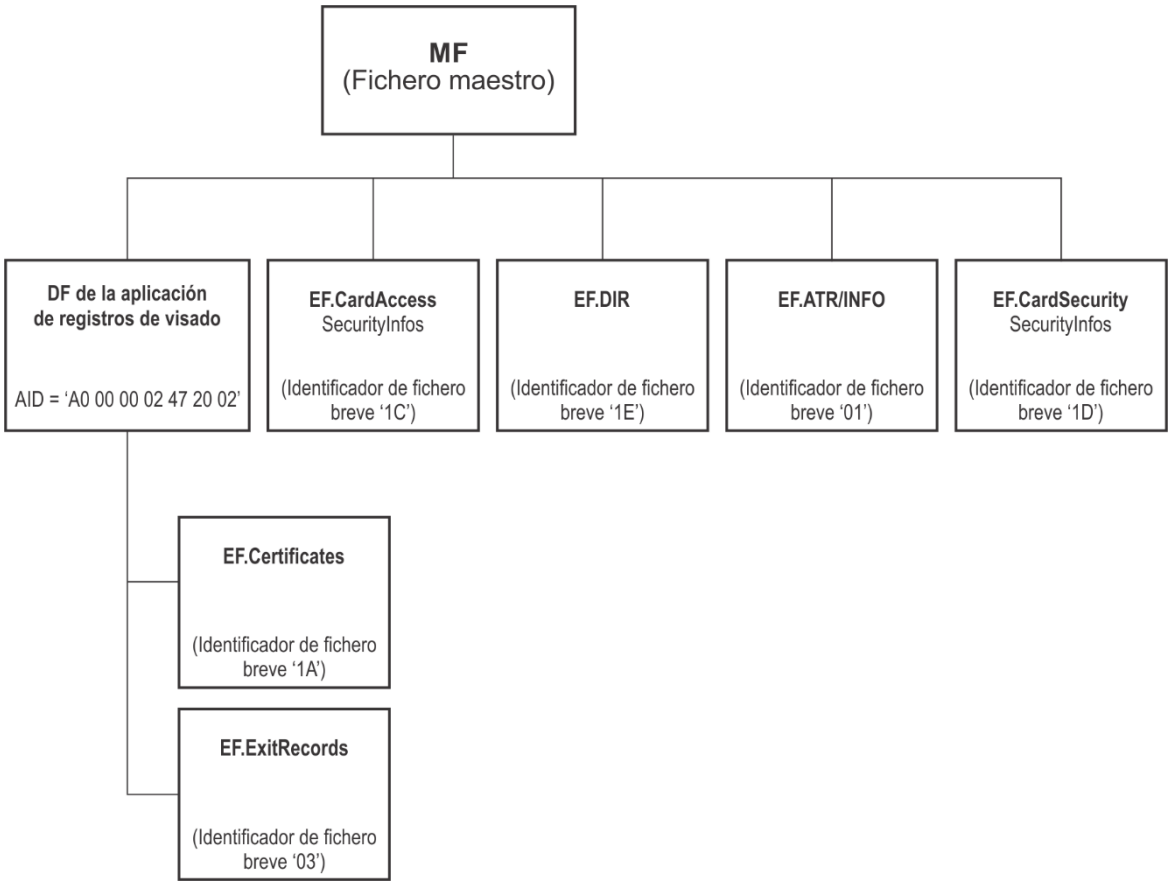


Figura 5. Estructura de los registros de visados

Los registros de visados se almacenan en el fichero elemental EF.VisaRecords en el DF de la aplicación de los registros de visados. El EF TENDRÁ una estructura lineal con registros de tamaño variable con arreglo a [ISO/IEC 7816-4]. Los certificados de firmante del registro de visados se almacenan en un fichero elemental separado EF.Certificates, que tiene una estructura lineal con registros de tamaño variable.

5.2.1 Selección de aplicación — DF

La aplicación de registros de visados DEBE seleccionarse utilizando el identificador de la aplicación (AID) como nombre DF reservado. El AID DEBE constar del identificador de la aplicación registrado asignado por la ISO con arreglo a [ISO/IEC 7816-5], seguido por la extensión de identificador de aplicación de propiedad (PIX) de la aplicación de registros de visados:

- el identificador de la aplicación registrado es 'A0 00 00 02 47';
- la aplicación de registros de visados DEBE usar PIX = '20 02'; y
- el AID completo de la aplicación de registros de visados DEBE ser 'A0 00 00 02 47 20 02'.

El IC DEBE rechazar la selección de esta aplicación si la autorización efectiva no garantiza derechos de acceso a ningún dato de una aplicación de la LDS2.

5.2.2 EF.Certificates (OBLIGATORIO)

Los certificados de firmante del registro de visado se almacenan en EF.Certificates dentro del DF de la aplicación y tienen una estructura lineal con registros de tamaño variable. Está previsto que el IS utilice estos certificados para realizar una nueva validación fuera de línea de la firma digital para cada registro del EF.VisaRecords.

Tabla 88. EF.Certificates

Nombre del fichero	EF.Certificates
ID del fichero	'011A'
Identificador EF breve	'1A'
Seleccionar / Acceso FMM	PACE+TA (Bit b3 de la autorización del registro de visado con arreglo a la tabla 97)
Acceso a Read record / Search Record (leer/buscar registro)	PACE+TA (Bit b3 de la autorización del registro de visado con arreglo a la tabla 97)
Acceso a Append Record (añadir registro)	PACE+TA (Bit b4 de la autorización del registro de visado con arreglo a la tabla 97)
Acceso a Write / Update Record (escribir/actualizar registro)	NUNCA
Acceso a Erase Record (borrar registro)	NUNCA
Estructura del fichero	Estructura lineal con registros de tamaño variable
Tamaño	Variable

El registro de certificado contiene un solo objeto de datos del certificado X.509 del firmante de la LDS2-TS. Un registro de certificado PUEDE constar como referencia en uno o más registros de visados.

La estructura del registro de certificado en la aplicación del visado es idéntica a la estructura del registro de certificado de la aplicación del registro de viaje que se especifica en la tabla 83.

Los registros de certificado se escriben en EF.Certificates, ubicado en el DF de la aplicación de registros de visados, usando el comando APPEND RECORD. Los registros de certificado pueden leerse de EF.Certificates utilizando el comando READ RECORD. Los registros de certificado NO DEBEN actualizarse ni borrarse. El número máximo de registros en EF.Certificates en el DF de la aplicación de registros de visados DEBE ser de 254.

5.2.3 EF.VisaRecords (OBLIGATORIO)

Los registros de visados DEBEN almacenarse en EF.VisaRecords, con una estructura lineal y registros de tamaño variable.

Tabla 89. EF.VisaRecords

Nombre del fichero	EF.VisaRecords
ID del fichero	‘0103’
Identificador EF breve	‘03’
Seleccionar / Acceso FMM	PACE+TA (Bit b1 de la autorización del registro de visado con arreglo a la tabla 97)
Acceso a Read record / Search Record (leer/buscar registro)	PACE+TA (Bit b1 de la autorización del registro de visado con arreglo a la tabla 97)
Acceso a Append Record (añadir registro)	PACE+TA (Bit b2 de la autorización del registro de visado con arreglo a la tabla 97)
Acceso a Write / Update Record (escribir/actualizar registro)	NUNCA
Acceso a Erase Record (borrar registro)	NUNCA
Estructura del fichero	Estructura lineal con registros de tamaño variable
Tamaño	Variable

Cada registro de visado DEBE contener una secuencia de objetos de datos BER-TLV (DO ‘5F28’ y DO’71’), seguida del DO testigo de autenticación (firma) y de un DO que contenga la referencia al certificado de firmante de la LDS2-V en EF.Certificates. DO’71’ contiene un conjunto de DO (campos), que se enumeran en la tabla que figura a continuación.

Nota.— Los rótulos interindustriales especificados en la tabla siguiente se usan en el contexto de la LDS, por lo que no es necesario un sistema de asignación de rótulos coexistentes.

Tabla 90. Formato EF.VisaRecords

Rótulo	Rótulo	Contenido	OBLIGATORIO/ OPCIONAL/ CONDICIONAL	Formato	Ejemplo
‘5F28’		Estado expedidor u organización expedidora (copia para SEARCH RECORD)	M	F (3) A	NLD
‘71’	Regostro de visado (información firmada)				
	‘5F28’	Estado expedidor u organización expedidora	M	F (3) A	NLD
	‘43’	Tipo de documento	M	F (2) A, N, S	VS
	‘5F71’	Visado de lectura mecánica del tipo A	O	F (48) A, N, S	

Rótulo	Rótulo	Contenido	OBLIGATORIO/ OPCIONAL/ CONDICIONAL	Formato	Ejemplo
	‘5F72’	Visado de lectura mecánica del tipo B	O	F (44) A, N, S	VCD<<DENT<<ARTHUR< PHILIP<<<<<<<<<<<
	‘5F73’	Número de entradas	O	V (1) B	‘01’ – ‘FF’
	‘5F74’	Duración de la estancia (días, meses, años)	O	F (3) B	‘010000’ – ‘FFFFFF’
	‘5F75’	Número de pasaporte	O	F (9) A, N, S	XI85935F8
	‘5F76’	Tipo de visado/clase/categoría	O	V (4) B	
	‘5F77’	Información del territorio	O	V (8) B	
	‘49’	Lugar de expedición (autoridad expedidora)	M	V (50) A, Sp	NUEVA YORK
	‘5F25’	Fecha efectiva (fecha de expedición)	M	F (8) N	20120826 (aaaammdd)
	‘5F24’	Fecha de caducidad	M	F (8) N	20130826 (aaaammdd)
	‘5A’	Número de documento	M	F (9) A, N, S	XI85935F8
	‘5F32’	Información adicional (aprobaciones: duración, limitaciones y derechos abonados)	O	V (50) A, N, S, U	Texto libre
	‘5B’	Nombre de la persona titular (nombre completo)	M	V (50) A, Sp	VAN DER STEEN MARIANNE LOUISE
	‘5F33’	Identificador primario (apellido)	M	V (50) A, Sp	VAN DER STEEN
	‘5F34’	Identificador secundario (nombre de pila)	M	V (50) A, Sp	MARIANNE LOUISE
	‘5F35’	Sexo	M	F (1) A, S	F, M, o <
	‘5F2B’	Fecha de nacimiento	M	F (8) N, S	19870814 (aaaammdd)
	‘5F2C’	Nacionalidad	M	F (3) A	NLD
	‘5F1F’	ZLM	M	V (50) A, N, S	VAN<DER<STEEN<< MARIANNE<LOUISE
	‘5F40’	Referencia al EF de aplicaciones biométricas	O	F (2) B	‘0201’
‘5F37’	Testigo de autenticación (firma)		M	V (140), B	‘5F’ ‘37’ Len {firma}
‘5F38’	Referencia (número de registro) al certificado de firmante de la LDS2-V en el almacén de certificados		M	F (1) B	‘01’ …’FE’

Nota 1.— A = carácter alfabético [a-z, A-Z], N = carácter numérico [0-9], S = carácter especial [‘<’], B= datos binarios, F = campo de longitud fija, Var = campo de longitud variable, Sp = espacio.

Nota 2.— Código de tres letras del Estado expedidor con arreglo al Doc 9303-3.

Nota 3.— Si el DO'5F40' opcional está presente, DEBE contener el identificador de dos bytes del EF dentro de la aplicación de datos biométricos adicionales que contiene los datos biométricos. Este DO solo puede usarse si la aplicación de los datos biométricos adicionales está presente en el eMRTD.

El orden de los objetos de datos de un registro es fijo. El IS DEBE establecer el contenido del registro utilizando los objetos de datos en el orden especificado en la tabla.

Cada registro de visado DEBE contener una firma digital (testigo de autenticación) calculada sobre el DO'71', incluidos el rótulo 71 y la longitud. La firma es generada por el firmante LDS2-V.

Los certificados de firmante de la LDS2-V exigidos para verificar la firma del registro de visado se almacenan en un almacén de EF.Certificates separado ubicado en el DF de la aplicación de registros de visados.

Cada registro de visado DEBE añadirse al EF.VisaRecords utilizando APPEND RECORD. Estos registros de visados NO DEBEN alterarse (actualizarse) ni borrarse. El número máximo de registros permitidos en EF.VisaRecords DEBE ser de 254.

5.3 Aplicación de los datos biométricos adicionales (CONDICIONAL)

La aplicación de los datos biométricos adicionales PUEDE ser implementada por un Estado expedidor o una organización expedidora. Si se ha invocado la aplicación de los datos biométricos adicionales opcional, o se ha referenciado en algún de registro de visado, SE EXIGE de forma condicional lo siguiente.

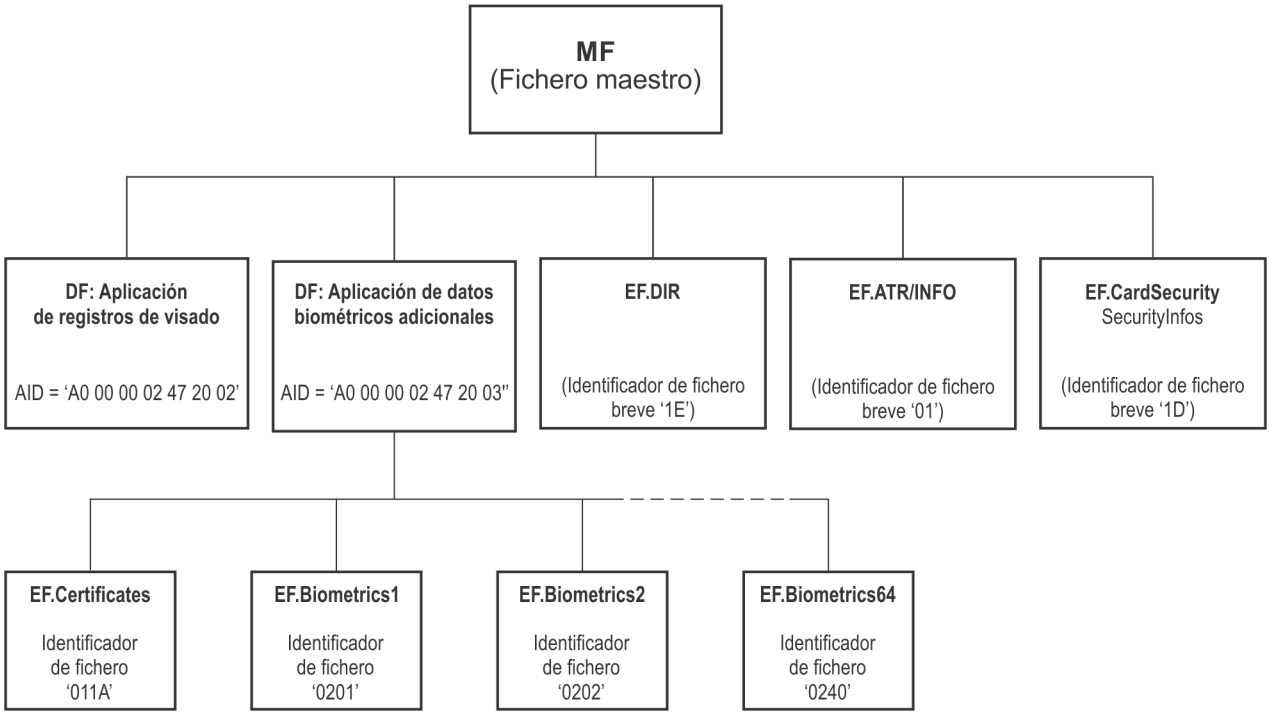


Figura 6. Estructura de la aplicación de los datos biométricos adicionales

5.3.1 Selección de aplicación — DF

La aplicación de los datos biométricos adicionales DEBE seleccionarse utilizando el identificador de la aplicación (AID) como nombre DF reservado. El AID DEBE constar del identificador de la aplicación registrado asignado por la ISO con arreglo a [ISO/IEC 7816-5], seguido por la extensión del identificador de aplicación de propiedad (PIX) de la aplicación de los datos biométricos adicionales:

- el identificador de la aplicación registrado es ‘A0 00 00 02 47’;
- la aplicación de los datos biométricos adicionales DEBE usar PIX = ‘20 03’; y
- el AID completo de la aplicación de los datos biométricos adicionales DEBE ser ‘A0 00 00 02 47 20 03’.

El CI DEBE rechazar la selección de esta aplicación si la autorización efectiva no garantiza derechos de acceso a ningún dato de una aplicación de la LDS2.

5.3.2 EF.Certificates (OBLIGATORIO)

Los certificados de firmante de los datos biométricos adicionales se almacenan en EF.Certificates dentro del DF de la aplicación y tienen una estructura lineal con registros de tamaño variable. Está previsto que el IS utilice estos certificados para realizar una nueva validación fuera de línea de la firma digital en el EF.Biometrics.

Tabla 91. EF.Certificates

Nombre del fichero	EF.Certificates
ID del fichero	‘011A’
Identificador EF breve	‘1A’
Seleccionar / Acceso FMM	PACE+TA (bit b1 del byte 1 de la autorización para la aplicación de datos biométricos adicionales (véase la tabla 98)
Acceso a Read record / Search Record (leer/buscar registro)	PACE+TA (bit b1 del byte 1 de la autorización para la aplicación de datos biométricos adicionales (véase la tabla 98)
Acceso a Append Record (añadir registro)	PACE+TA (bit b2 del byte 1 de la autorización para la aplicación de datos biométricos adicionales (véase la tabla 98)
Acceso a Write / Update Record (escribir/actualizar registro)	NUNCA
Acceso a Erase Record (borrar registro)	NUNCA
Estructura del fichero	Estructura lineal con registros de tamaño variable
Tamaño	Variable

El registro de certificado contiene un solo objeto de datos del certificado X.509 del firmante de los datos biométricos adicionales. Un registro de certificado PUEDE constar como referencia en uno o más EF de datos biométricos adicionales.

La estructura del registro de certificado en la aplicación de los datos biométricos adicionales es idéntica a la estructura del registro de certificado de la aplicación de los registros de viaje que se especifica en la tabla 83.

Los registros de certificado se escriben en EF.Certificates, ubicado en el DF de la aplicación de datos biométricos adicionales, usando el comando APPEND RECORD. Los registros de certificado pueden leerse de EF.Certificates utilizando el comando READ RECORD. Los registros de certificado NO DEBEN actualizarse ni borrarse. El número máximo de registros en EF.Certificates en el DF de la aplicación de las datos biométricos adicionales DEBE ser de 64.

5.3.3 EF.Biometrics

Los datos biométricos adicionales DEBEN almacenarse en EF de la aplicación de datos biométricos adicionales y tener una estructura transparente conforme a [ISO/IEC 7816-4].

Cada EF de datos biométricos PUEDE vincularse a uno o más registros de EF.VisaRecords en la aplicación de registros de visados (u otros EF y aplicaciones) por medio del identificador EF de datos biométricos adicionales.

Tabla 92. EF.Biometrics1 a EF.Biometrics64

Nombre del fichero	EF.Biometrics1 a EF.Biometrics64
ID del fichero	‘0201’ a ‘0240’
Identificador EF breve	N/A
Select / FMM / Read Access in Deactivated state	PACE+TA (autorización AdditionalBiometrics con arreglo a la tabla 98, bits b2, b4, b6, b8 de los bytes 2-17)
Acceso de escritura en el estado desactivado	PACE+TA (autorización AdditionalBiometrics con arreglo a la tabla 98, bits b2, b4, b6, b8 de los bytes 2-17)
Activar el acceso en el estado desactivado	PACE+TA (autorización AdditionalBiometrics con arreglo a la tabla 98, bits b2, b4, b6, b8 de los bytes 2-17)
Seleccionar / FMM / Acceso de lectura en el estado activado	PACE+TA (autorización AdditionalBiometrics con arreglo a la tabla 98, bits b1, b3, b5, b7 de los bytes 2-17)
Acceso de escritura en el estado activado	NUNCA
Activar el acceso en el estado activado	NUNCA
Borrar el acceso	NUNCA
Estructura del fichero	Estructura transparente
Tamaño	Variable

Cada EF de datos biométricos adicionales DEBE contener un objeto de datos DO'7F2E' en BER-TLV que encapsule tres objetos de datos: el objeto de datos biométricos DO'5F2E', seguido de los DO'5F37' y DO'5F38' de testigo de autenticación (firma) que contienen la referencia a un certificado de firmante de los datos biométricos adicionales en EF.Certificates, como se muestra en la tabla que figura a continuación.

El contenido del DO'5F2E' depende del expedidor de los datos biométricos adicionales y queda fuera del alcance de esta especificación.

El mecanismo de creación del EF de datos biométricos adicionales queda fuera del alcance de esta especificación. El expedidor DEBERÍA crear previamente varios EF de datos biométricos adicionales.

Nota.— Los rótulos interindustriales especificados en la tabla que figura a continuación se usan en el contexto de la LDS, por lo que no es necesario un sistema de asignación de rótulos coexistentes.

Tabla 93. Formato EF.Biometrics

Rótulo	Rótulo	Contenido	OBLIGATORIO/ OPCIONAL/ CONDICIONAL	Formato	Ejemplo
'7F2E'		Plantilla de datos biométricos	M		'7F' '2E' Len {DO'5F2E' || DO'5F37' || DO'5F38'}
	'5F2E'	Datos biométricos adicionales	M	V, B	'5F' '2E' Len {Datos biométricos}
	'5F37'	Testigo de autenticación (firma)	M	V (140), B	'5F' '37' Len {Firma}
	'5F38'	Referencia (número de registro) al certificado de firmante de los datos biométricos adicionales en el almacén de certificados	M	F (1) B	'01' …'40'

Nota.— B = datos binarios, F = campo de longitud fija, V = campo de longitud variable.

El orden de los objetos de datos de un EF es fijo.

Cada EF de datos biométricos adicionales DEBE contener una firma digital (testigo de autenticación) calculada sobre el DO'5F2E', incluidos el rótulo y la longitud. La firma la genera el firmante de los datos biométricos adicionales.

El certificado del firmante de las datos biométricos adicionales necesario para verificar la firma de las datos biométricos adicionales se almacena en un almacén de EF.Certificates separado ubicado en el DF de la aplicación de las datos biométricos adicionales.

Cada EF de datos biométricos adicionales DEBE escribirse utilizando el comando UPDATE BINARY.

El EF de datos biométricos adicionales NO DEBE alterarse (actualizarse) ni borrarse. El número máximo de EF de datos biométricos adicionales es de 64.

En la tabla 94 figuran todos los posibles nombres de EF de datos biométricos adicionales, identificadores EF e identificadores EF breves.

Tabla 94. Identificadores EF.Biometrics

Nombre de EF	Identificador EF	Identificador EF breve
EF.Biometrics1	‘0201’	N/A
EF.Biometrics2	‘0202’	N/A
EF.Biometrics3	‘0203’	N/A
EF.Biometrics4	‘0204’	N/A
EF.Biometrics5	‘0205’	N/A
EF.Biometrics6	‘0206’	N/A
EF.Biometrics7	‘0207’	N/A
EF.Biometrics8	‘0208’	N/A
EF.Biometrics9	‘0209’	N/A
EF.Biometrics10	‘020A’	N/A
EF.Biometrics11	‘020B’	N/A
EF.Biometrics12	‘020C’	N/A
EF.Biometrics13	‘020D’	N/A
EF.Biometrics14	‘020E’	N/A
EF.Biometrics15	‘020F’	N/A
EF.Biometrics16	‘0210’	N/A
EF.Biometrics17	‘0211’	N/A
EF.Biometrics18	‘0212’	N/A
EF.Biometrics19	‘0213’	N/A
EF.Biometrics20	‘0214’	N/A
EF.Biometrics21	‘0215’	N/A
EF.Biometrics22	‘0216’	N/A
EF.Biometrics23	‘0217’	N/A
EF.Biometrics24	‘0218’	N/A
EF.Biometrics25	‘0219’	N/A
EF.Biometrics26	‘021A’	N/A
EF.Biometrics27	‘021B’	N/A
EF.Biometrics28	‘021C’	N/A
EF.Biometrics29	‘021D’	N/A
EF.Biometrics30	‘021E’	N/A
EF.Biometrics31	‘021F’	N/A
EF.Biometrics32	‘0220’	N/A

Nombre de EF	Identificador EF	Identificador EF breve
EF.Biometrics33	‘0221’	N/A
EF.Biometrics34	‘0222’	N/A
EF.Biometrics35	‘0223’	N/A
EF.Biometrics36	‘0224’	N/A
EF.Biometrics37	‘0225’	N/A
EF.Biometrics38	‘0226’	N/A
EF.Biometrics39	‘0227’	N/A
EF.Biometrics40	‘0228’	N/A
EF.Biometrics41	‘0229’	N/A
EF.Biometrics42	‘022A’	N/A
EF.Biometrics43	‘022B’	N/A
EF.Biometrics44	‘022C’	N/A
EF.Biometrics45	‘022D’	N/A
EF.Biometrics46	‘022E’	N/A
EF.Biometrics47	‘022F’	N/A
EF.Biometrics48	‘0230’	N/A
EF.Biometrics49	‘0231’	N/A
EF.Biometrics50	‘0232’	N/A
EF.Biometrics51	‘0233’	N/A
EF.Biometrics52	‘0234’	N/A
EF.Biometrics53	‘0235’	N/A
EF.Biometrics54	‘0236’	N/A
EF.Biometrics55	‘0237’	N/A
EF.Biometrics56	‘0238’	N/A
EF.Biometrics57	‘0239’	N/A
EF.Biometrics58	‘023A’	N/A
EF.Biometrics59	‘023B’	N/A
EF.Biometrics60	‘023C’	N/A
EF.Biometrics61	‘023D’	N/A
EF.Biometrics62	‘023E’	N/A
EF.Biometrics63	‘023F’	N/A
EF.Biometrics64	‘0240’	N/A

5.4 Condiciones de acceso al fichero de la aplicación de la LDS2 (CONDICIONAL)

5.4.1 Funciones y niveles de autorización por defecto (OBLIGATORIO)

Cada certificado CV contiene una plantilla de autorización de la persona titular del certificado (CHAT) que identifica la función del titular del certificado (IS, DV, CVCA) y contiene derechos de acceso a DG3/DG4 de la aplicación de la LDS2 del eMRTD EXIGIDA (debido a usos heredados u otros usos nacionales).

CHAT comprende una secuencia de dos objectos

a) Un identificador de objetos que especifique el tipo de terminal y el formato de la plantilla [TR- 03110]:

```
id-roles OBJECT IDENTIFIER ::= {bsi-de applications(3) mrtd(1) 2}
id-IS       OBJECT IDENTIFIER ::= {id-roles 1}
```

b) Un objeto de datos discrecional (rótulo '53') que contenga la función codificada en bits y derechos de acceso de solo lectura de la persona titular del certificado con arreglo a la siguiente tabla:

Tabla 95. Autorización CHAT por defecto

		Byte 1							
	Descripción	**b8**	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**
Función	CVCA	1	1						
	DV (nacional)	1	0						
	DV (extranjero)	0	1						
	IS	0	0						
Acceso de lectura	RFU								
	RFU								
	RFU								
	RFU								
	DG4 (iris)							1	
	DG3 (dedo)								1

Nota.— La LDS2 para el eMRTD NO DEBE tener en cuenta el valor de los bits RFU de la autorización de la persona titular del certificado.

5.4.2 Niveles de autorización de la aplicación (OBLIGATORIO)

Las autorizaciones de personas titulares de certificados para cada aplicación de la LDS2 se codifican con extensiones de certificado CV (una extensión por aplicación). La extensión de certificado es una plantilla discrecional (rótulo '73') que comprende dos objetos de datos: un identificador de objeto de autorización (rótulo '06') para una aplicación específica y un objeto de datos discrecional (rótulo '53') que contenga derechos de acceso codificados en bits de la persona titular del certificado a una aplicación especificada.

Para determinar la autorización efectiva de una persona titular de un certificado, la LDS2 para la microplaqueta del eMRTD calcula un operador booleano "Y" a nivel de bit de los derechos de acceso contenidos en las extensiones del certificado IS y los certificados DV y CVCA de referencia.

Para la aplicación de los registros de viaje, los identificadores de objeto de autorización y las codificaciones de derechos de acceso son las siguientes:

```
id-icao-lds2-travelRecords       OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER::= {id-icao-lds2-
travelRecords 3}
```

Tabla 96. Autorizaciones para la aplicación de los registros de viaje

	Descripción	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Derechos de acceso	RFU								
	RFU								
	RFU								
	RFU								
	Añadir EF.Certificates					1			
	Leer/Buscar/Seleccionar/ EF.Certificates FMM						1		
	Añadir EF.EntryRecords/ExitRecords							1	
	Leer/Buscar/Seleccionar/EF.EntryRecords/ExitRecords FMM								1

Para la aplicación de los registros de visado, los identificadores de objeto de autorización y las codificaciones de derechos de acceso son los siguientes:

```
id-icao-lds2-visaRecords         OBJECT IDENTIFIER ::= {id-icao-lds2 2}

id-icao-lds2-visaRecords-access OBJECT IDENTIFIER  ::= {id-icao-lds2-
visaRecords 3}
```

Tabla 97. Autorizaciones para la aplicación de los registros de visado

	Descripción	Byte 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Derechos de acceso	RFU								
	RFU								
	RFU								
	RFU								
	Añadir EF.Certificates					1			
	Leer/Buscar/Seleccionar/EF.Certificates FMM						1		
	Añadir EF.VisaRecords							1	
	Leer/Buscar/Seleccionar/EF.VisaRecords FMM								1

Para la aplicación de datos biométricos adicionales, los identificadores de objeto de autorización y las codificaciones de derechos de acceso son las siguientes:

```
id-icao-lds2-additionalBiometricsOBJECT IDENTIFIER ::= {id-icao-lds2 3}

id-icao-lds2-additionalBiometrics-access  OBJECT  IDENTIFIER::=  {id-icao-lds2-
additionalBiometrics 3}
```

Tabla 98. Autorizaciones para la aplicación de datos biométricos adicionales

	Descripción	Identificador EF	Autorizaciones							
			b8	b7	b6	b5	b4	b3	b2	b1
Byte 1	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	Añadir EF.Certificates	'011A'							1	
	Seleccionar/FMM/Leer/Buscar EF.Certificates	'011A'								1
Byte 2	Seleccionar/FMM/Escribir/Activar/Leer EF.Biometrics1 en estado desactivado	'0201'	1							
	Seleccionar/FMM/Leer EF.Biometrics1 en estado activado	'0201'		1						
	Seleccionar/FMM/Escribir/Activate/Read EF.Biometrics2 en estado desactivado	'0202'			1					
	Seleccionar/FMM/Read EF.Biometrics2 en estado activado	'0202'				1				
	Seleccionar/FMM/ Escribir/Activate/Read EF.Biometrics3 en estado desactivado	'0203'					1			
	Seleccionar/FMM/Read EF.Biometrics3 en estado activado	'0203'						1		
	Seleccionar/FMM/ Escribir/Activate/Read EF.Biometrics4 en estado desactivado	'0204'							1	
	Seleccionar/FMM/Read EF.Biometrics4 en estado activado	'0204'								1
	...									
Byte 17	Seleccionar/FMM/Escribir/Activate/Leer EF.Biometrics61 en estado desactivado	'023D'	1							
	Seleccionar/FMM/Leer EF.Biometrics61 en estado activado	'023D'		1						
	Seleccionar/FMM/Write/Activate/Leer EF.Biometrics62 en estado desactivado	'023E'			1					
	Seleccionar/FMM/Leer EF.Biometrics62 en estado activado	'023E'				1				
	Seleccionar/FMM/Escribir/Activate/Read EF.Biometrics63 en estado desactivado	'023F'					1			
	Seleccionar/FMM/Leer EF.Biometrics63 en estado activado	'023F'						1		
	Seleccionar/FMM/Escribir/Activate/Leer EF.Biometrics64 en estado desactivado	'0240'							1	
	Seleccionar/FMM/Leer EF.Biometrics64 en estado activado	'0240'								1

Nota 1.— La LDS2 para el eMRTD NO DEBE tener en cuenta el valor de los bits RFU en la autorización de la persona titular del certificado.

Nota 2.— Los Estados expedidores u organizaciones expedidoras NO DEBEN expedir certificados de terminal con autorizaciones para escribir/activar el IS si solo tienen autorizaciones de lectura para las datos biométricos adicionales.

6. IDENTIFICADORES DE OBJETO

6.1 Resumen de los identificadores de objeto de las aplicaciones de la LDS1 y LDS2

Tabla 99. OID de LDS1.7, LDS1.8 y LDS2

Identificador de objeto	Valor	Comentario
id-icao	joint-iso-itu-t(2) international-organizations(23) icao(136)	OID de la OACI
id-icao-mrtd	id-icao 1	OID del eMRTD
id-icao-mrtd-security	id-icao-mrtd 1	
id-icao-ldsSecurityObject	id-icao-mrtd-security 1	Objeto de seguridad de LDS
id-icao-mrtd-security-cscaMasterList	id-icao-mrtd-security 2	Lista maestra de CSCA
id-icao-mrtd-security-cscaMasterListSigningKey	id-icao-mrtd-security 3	
id-icao-mrtd-security-documentTypeList	id-icao-mrtd-security 4	Lista de tipos de documento
id-icao-mrtd-security-aaProtocolObject	id-icao-mrtd-security 5	Protocolo de autenticación activa
id-icao-mrtd-security-extensions	id-icao-mrtd-security 6	Cambio de nombre de la CSCA
id-icao-mrtd-security-extensions-nameChange	id-icao-mrtd-security-extensions 1	
id-icao-mrtd-security-extensions-documentTypeList	id-icao-mrtd-security-extensions 2	Tipo de documento DS
id-icao-mrtd-security-DeviationList	id-icao-mrtd-security 7	OID de base de la lista de defectos
id-icao-mrtd-security-DeviationListSigningKey	id-icao-mrtd-security 8	
id-icao-lds2	id-icao-mrtd-security 9	Identificadores de objetos LDS2
id-icao-lds2-travelRecords	id-icao-lds2 1	OID de la base de aplicación de los registros de viaje
id-icao-lds2-travelRecords-application	id-icao-lds2-travelRecords 1	AID de la aplicación de los registros de viaje
id-icao-lds2-travelRecords-access	id-icao-lds2-travelRecords 3	Extensión de certificado de autorización
id-icao-lds2-visaRecords	id-icao-lds2 2	OID de la base de aplicación de los registros de visado
id-icao-lds2-visaRecords-application	id-icao-lds2-visaRecords 1	AID de los registros de visado
id-icao-lds2-visaRecords-access	id-icao-lds2-visaRecords 3	Extensión del certificado de autorización
id-icao-lds2-additionalBiometrics	id-icao-lds2 3	OID de la base de los datos biométricos adicionales
id-icao-lds2-additionalBiometrics-application	id-icao-lds2-additionalBiometrics 1	AID de los datos biométricos adicionales

Identificador de objeto	Valor	Comentario
id-icao-lds2-additionalBiometrics-access	id-icao-lds2-additionalBiometrics 3	Extensión del certificado de autorización
id-icao-lds2Signer	id-icao-lds2 8	Identificadores de objetos de firmante LDS2
id-icao-tsSigner	id-icao-lds2Signer 1	Certificado de firmante del sello de viaje LDS2
id-icao-vSigner	id-icao-lds2Signer 2	Certificado de firmante del visado LDS2
id-icao-bSigner	id-icao-lds2Signer 3	Certificado de firmante de los datos biométricos adicionales LDS2
id-icao-spoc	id-icao-mrtd-security 10	Identificadores de objeto de SPOC
id-icao-spocClient	id-icao-spoc 1	Cliente
id-icao-spocServer	id-icao-spoc 2	Servidor

7. ESPECIFICACIONES ASN.1

```
id-icao OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) international-organizations(23)
icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 2}
id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 3}
id-icao-mrtd-security-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-security
4}
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security
5}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-mrtd-
security-extensions 1}
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-
security-extensions 2}
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 8}

id-icao-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}
```

Identificadores de objeto de las aplicaciones de los registros de viaje LDS2

```
id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 3}
```

Identificadores de objeto de las aplicaciones de los registros de visado LDS2

```
id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 1}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 3}
```

Identificadores de objeto de las aplicaciones de datos biométricos adicionales LDS2

```
id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}
id-icao-lds2-additionalBiometrics-application OBJECT IDENTIFIER ::= {id-icao-lds2-additionalBiometrics 1}
id-icao-lds2-additionalBiometrics-access OBJECT IDENTIFIER ::= {id-icao-lds2-additionalBiometrics 3}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-lds2 8}
id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}
id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}
id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}
id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}
id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}
```

8. REFERENCIAS (NORMATIVA)

ISO/IEC 14443-1	ISO/IEC 14443-1:2016, *Tarjetas de identidad — Tarjetas de circuitos integrados sin contacto — Tarjetas de proximidad — Parte 1: Características físicas*
ISO/IEC 14443-2	ISO/IEC 14443-2:2016, *Tarjetas de identidad — Tarjetas de circuitos integrados sin contacto — Tarjetas de proximidad — Parte 2: Potencia e interfaz de señales de radiofrecuencia*
ISO/IEC 14443-3	ISO/IEC 14443-3:2016, *Tarjetas de identidad — Tarjetas de circuitos integrados sin contacto — Tarjetas de proximidad — Parte 3: Inicialización y anticolisión*
ISO/IEC 14443-4	ISO/IEC 14443-4:2016, *Tarjetas de identidad — Tarjetas de circuitos integrados sin contacto — Tarjetas de proximidad — Parte 4: Protocolo de transmisión*
ISO/IEC 10373-6	ISO/IEC 10373-6:2016, *Tarjetas de identidad — Métodos de ensayo — Parte 6: Tarjetas de proximidad*
ISO/IEC 18745-2	ISO/IEC 18745-2:2016, *Tecnología de la información Métodos de ensayo para documentos de viaje de lectura mecánica (MRTD) y dispositivos asociados - Parte 2: Métodos de ensayo para la interfaz sin contacto*
ISO/IEC 7816-2	ISO/IEC 7816-2: 2007, *Tarjetas de identidad — Tarjetas de circuito integrado — Parte 2: Tarjetas con contacto — Dimensiones y ubicación de los contactos*
ISO/IEC 7816-4	ISO/IEC 7816-4: 2013, *Tarjetas de identidad — Tarjetas de circuitos integrados —*

	Parte 4: Organización, seguridad y órdenes para el intercambio
ISO/IEC 7816-5	ISO/IEC 7816-5: 2004, *Tarjetas de identidad — Tarjetas de circuitos integrados — Parte 5: Registro de proveedores de aplicaciones*
ISO/IEC 7816-6	ISO/IEC 7816-6: 2016, *Tarjetas de identidad — Tarjetas de circuitos integrados — Parte 6: Elementos de datos interindustria para intercambio (incluido informe de defecto)*
ISO/IEC 7816-11	ISO/IEC 7816-11: 2017, *Tarjetas de identidad — Tarjetas de circuitos integrados — Parte 11: Verificación personal mediante métodos biométricos*
ISO/IEC 8825-1	ISO/IEC 8825-1:2008, *Tecnología de la información — Reglas de codificación ASN.1: Especificación de reglas básicas de codificación (BER), Reglas de codificación canónicas (CER) y Reglas de codificación distinguidas (DER)*
ISO/IEC 19794-4	ISO/IEC 19794-4:2005, *Tecnología de la información — Formatos de intercambio de datos biométricos — Parte 4: Datos de imágenes del dedo*
ISO/IEC 19794-5	ISO/IEC 19794-5:2005*, Tecnología de la información — Formatos de intercambio de datos biométricos — Parte 5: Datos de imágenes del rostro*
ISO/IEC 19794-6	ISO/IEC 19794-6:2011, Tecnología de la información — Formato de intercambio de datos biométricos — Parte 6: Datos de imágenes del iris
ISO/IEC 10646	ISO/IEC 10646:2012*, Tecnología de la información — Conjunto universal de caracteres codificados en octetos múltiples (UCS)*
RFC 3369	Sintaxis de mensajes criptográficos 2002
ISO/IEC 10918-1	ISO/IEC 10918-1:1994, *Tecnología de la información — Compresión y codificaciones digitales de imágenes fijas de tono continuo: Requisitos y directrices*
ISO/IEC 15444	ISO/IEC 15444-n, *Sistema de codificación de imágenes JPEG 2000*
ISO/IEC 19785	ISO/IEC 19785-n, *Tecnología de la información — Marco común de formatos de intercambio biométrico*
ISO/IEC 19795-6	ISO/IEC 19795-6:2012, *Tecnología de la información — Informes y pruebas de rendimiento biométrico — Parte 6: Métodos de prueba para la evaluación operativa*
ISO/IEC 39794-4	ISO/IEC 39794-4:2019, *Tecnología de la información— Formatos de intercambio de datos biométricos extensibles — Parte 4: Datos de imágenes del dedo*
ISO/IEC 39794-5	ISO/IEC 39794-5:2019, *Tecnología de la información — Formatos de intercambio de datos biométricos extensibles — Parte 5: Datos de imágenes del rostro*
ISO/IEC 39794-6	ISO/IEC 39794-6:2021, *Tecnología de la información — Formatos de intercambio de datos biométricos extensibles — Parte 6: Datos de imágenes del iris*

— — — — — — — —

Apéndice A de la Parte 10

EJEMPLOS DE CORRESPONDENCIAS EN LA ESTRUCTURA LÓGICA DE DATOS (INFORMATIVO)

El siguiente texto informativo describe ejemplos de correspondencias de la estructura lógica de datos (LDS v1.7) utilizando una representación de acceso aleatorio a un circuito integrado sin contacto en un eMRTD.

A.1 DATOS COMUNES DE EF.COM

El ejemplo siguiente indica una implantación de LDS Versión 1.7 utilizando la versión 4.0.0 de Unicode con grupos de datos 1 (rótulo '61'), 2 (rótulo '75'), 4 (rótulo '76') y 12 (rótulo '6C') presentes.

Para éste y todos los demás ejemplos, los rótulos se imprimen en **negrita**, las longitudes de imprimen en *bastardilla*, y los valores se imprimen en tipo romano. Los rótulos hexadecimales, longitudes y valores se indican entre comillas ('xx').

'60' *'16'*
'5F01' *'04'* '0107'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

El ejemplo se leería en representación hexadecimal completa como:

'60' *'16'*
'5F01' *'04'* '30313037'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

Una hipotética LDS versión 15.99 se codificaría como:

'60' *'16'*
'5F01' *'04'* '1599'
'5F36' *'06'* '040000'
'5C' *'04'* '6175766C'

o hexadecimal:

'60' *'16'*
'5F01' *'04'* '31353939'
'5F36' *'06'* '303430303030'
'5C' *'04'* '6175766C'

A.2 INFORMACIÓN DE LA ZONA DE LECTURA MECÁNICA EF.DG1

A.2.1 eMRTD de tamaño DV1

A continuación se muestra un ejemplo del DG1 que utiliza esta información en una LDS1 de un eMRTD de tamaño DV1. La longitud del dato en la ZLM es 90 bytes (‘5A’).

‘61’ *‘5D’* **‘5F1F’** *‘5A’*

```
I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARI
ANNE<LOUISE
```

A.2.2 eMRTD de tamaño DV2

A continuación se muestra un ejemplo del DG1 que utiliza esta información en una LDS1 de un eMRTD de tamaño DV2. La longitud del dato en la ZLM es 72 bytes (‘48’).

‘61’ *‘4B’* **‘5F1F’** *‘48’*

```
I<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<54
```

A.3 PLANTILLAS BIOMÉTRICAS PARA EF.DG2 A EF.DG4

Los DG2 a DG4 utilizan la opción fuera de tarjeta anidada en [ISO/IEC 7816-11], para tener la posibilidad de almacenar múltiples plantillas biométricas de un tipo que se correspondan con el marco común de formatos de intercambio biométrico (CBEFF), NISTR 6529a. El subencabezamiento biométrico define el tipo de característica biométrica presente y la característica biométrica específica.

Ejemplo: una característica biométrica del rostro, firmada, con longitud de bloque de datos de 12 642 bytes (‘3162’ bytes), codificada utilizando un dispositivo con una PID de ‘00 01 00 01’, tipo de formato ‘00 04’ propiedad del proveedor de plantilla ‘00 0A’ fue captada el 15 de marzo de 2002 (sin desplazamiento UTC) y es válida del 1 de abril de 2002 hasta el 31 de marzo de 2007. Se utiliza la versión 1.0 de la plantilla patrón de la OACI.

La longitud total de la plantilla es 12 704 bytes. La plantilla se almacena iniciándose al comienzo de EF.DG2 (SFID 02).

‘75’ *‘82319EC’*
- **‘7F61’** *‘823199’*
  - **‘02’** *‘01’* ‘01’
  - **‘7F60’** *‘823191’*
  - **‘A1’** *‘26’*
    - **‘80’** *‘02’* ‘0101’
    - **‘81’** *‘01’* ‘02’
    - **‘83’** *‘07’* ‘20020315133000’
    - **‘85’** *‘08’* ‘2002040120070331’
    - **‘86’** *‘04’* ‘00010001’
    - **‘87’** *‘02’* ‘0101’
    - **‘88’** *‘02’* ‘0008’
  - **‘5F2E’** *‘823162’* ‘… 12 642 bytes de datos biométricos …’

A.4 PLANTILLAS DE IMAGEN EXHIBIDA DE EF.DG5 A EF.DG7

Nota.—Un EF por cada DG.

Ejemplo: plantilla de imagen con longitud de datos de imagen exhibida de 2 000 bytes. La longitud de la plantilla es 2 008 bytes (‘07D8’).

‘65’ *‘8207D8’*
‘02’ *‘01’* 1
‘5F40’ *‘8207D0’* ‘….2 000 bytes de datos de imagen …’

A.5 Detalles personales adicionales EN EF.DG11

El ejemplo a continuación muestra los siguientes detalles personales: Nombre completo (John J. Smith), Lugar de nacimiento (Anytown, MN), Dirección permanente (123 Maple Rd, Anytown, MN), Número de teléfono 1-612-555-1212 y Profesión (agente de viajes-travel agent). La longitud de la plantilla es 99 bytes (*‘63’*).

‘6B’ *‘63’*
‘5C’ *‘0A’* **‘5F0E’ ‘5F11’ ‘5F42’ ‘5F12’ ‘5F13’**
‘5F0E’ *‘0D’* SMITH<<JOHN<J
‘5F11’ *‘0A’* ANYTOWN<MN
‘5F42’ *‘17’* 123 MAPLE RD<ANYTOWN<MN
‘5F12’ *‘0E’* 16125551212
‘5F13’ *‘0C’* TRAVEL<AGENT

A.6 PERSONAS QUE HAN DE NOTIFICARSE EN EF.DG16

Ejemplo con dos entradas: Charles R. Smith de Anytown, MN y Mary J. Brown of Ocean Breeze, CA. La longitud de la plantilla es 162 bytes (‘A2’).

‘70’ *‘81A2’*

‘02’ *‘01’* 2
‘A1’ ‘4C’
‘5F50’ *‘08’* 20020101
‘5F51’ *‘10’* SMITH<<CHARLES<R
‘5F52’ *‘0B’* 19525551212
‘5F53’ *‘1D’* 123 MAPLE RD<ANYTOWN<MN<55100
‘A2’ ‘4F’
‘5F50’ *‘08’* 20020315
‘5F51’ *‘0D’* BROWN<<MARY<J
‘5F52’ *‘0B’* 14155551212
‘5F53’ *‘23’* 49 REDWOOD LN<OCEAN BREEZE<CA<94000

— — — — — — — —

Apéndice B de la Parte 10

CI SIN CONTACTO DE UN eMRP (INFORMATIVO)

B.1 TAMAÑO Y CLASE DE LA ANTENA DE UN eMRTD

El Estado expedidor establece el tamaño de antena según su propio criterio. A excepción del tamaño de la antena, tanto la LDS1 como la LDS2 del eMRTD superarán satisfactoriamente todos los ensayos especificados en [ISO/IEC 18745-2] aplicando las especificaciones de clase 1.

Se RECOMIENDA que los eMRTD sean también conformes con las especificaciones de la Clase 1.

No se establece una posición obligatoria para el CI, que PUEDE ubicarse en cualquier posición. La situación de la antena sin contacto es discrecional del Estado expedidor, pero siempre en una de las posiciones siguientes:

Página de datos — el CI y la antena se incluyen en la estructura de una página de datos que es página interna,
Central en el cuadernillo — el CI y la antena se colocan entre las páginas centrales del cuadernillo,
Tapa — se sitúa en la estructura o diseño constructivo de la tapa,
Página separada cosida — el CI y su antena se incluyen en una página separada que PUEDE tener la forma de una tarjeta de plástico de tamaño ID-3 cosida al cuadernillo durante el proceso de fabricación, o
Contratapa — se sitúa en la estructura o diseño constructivo de la tapa trasera del cuadernillo.

B.2 ARRANQUE E INTERROGACIÓN

Un eMRTD expuesto a un campo magnético alterno de 1,5 A/m medido con arreglo a [ISO/IEC 18745-2] responderá a cualquier REQ/WUP que sea adecuada a su tipo tras una exposición a un campo magnético alterno no modulado de 10 m. Se RECOMIENDA que pueda responder a cualquier REQ/WUP adecuada a su tipo tras una exposición al campo magnético alterno no modulado de 5 ms.

B.3 ANTICOLISIÓN Y TIPO

El eMRTD PUEDE ser conforme con el Tipo A o el Tipo B definidos en [ISO/IEC 14443-2]. Ello no modificará su tipo salvo que sea reinicializado por el sistema de inspección asociado al eMRTD.

B.4 VELOCIDADES BINARIAS OBLIGATORIAS

El eMRTD proporcionará obligatoriamente, al menos, las velocidades binarias siguientes definidas en [ISO/IEC 14443-2]: 106 kbit/s y 424 kbit/s en ambos sentidos entre el eMRTD y el sistema de inspección asociado al eMRTD.

La velocidad binaria de 212 kbit/s, y todas las velocidades binarias desde 848 kbit/s hasta 6,78 Mbit/s en ambos sentidos, y de 10,17 Mbit/s a 27.12 Mbit/s desde el sistema de inspección del eMRTD al eMRTD, tal como se define en [ISO/IEC 14443-2], son opcionales.

B.5 PERTURBACIÓN ELECTROMAGNÉTICA (EMD)

No es obligatorio admitir la EMD.

Nota.— La característica EMD mejora la robustez de la comunicación sin contacto entre el eMRTD y el sistema de inspección asociado al eMRTD contra la perturbación electromagnética generada por el propio eMRTD. El consumo de corriente dinámica del eMRTD durante la ejecución de una instrucción puede tener un efecto aleatorio de modulación de la carga (que puede no ser puramente resistiva) sobre el campo magnético. En algunos casos, el sistema de inspección asociado al eMRTD puede interpretar erróneamente la EMD como datos enviados por el eMRTD, lo que puede afectar negativamente a la recepción adecuada de la respuesta del eMRTD.

B.6 ADMISIÓN DEL INTERCAMBIO DE PARÁMETROS ADICIONALES (OPCIONAL)

El eMRTD PUEDE admitir el intercambio de parámetros adicionales definidos en [ISO/IEC 14443-4] al objeto de negociar velocidades binarias superiores a 106 kbit/s. También PUEDE utilizar los mismos parámetros adicionales para negociar tramas con corrección de errores, tal como se especifica en [ISO/IEC 14443-4].

B.7 APANTALLAMIENTO

Se RECOMIENDA no apantallar ninguna página del eMRTD.

B.8 IDENTIFICADOR ÚNICO (UID) E IDENTIFICADOR PICC PSEUDOÚNICO (PUPI) (RECOMENDADO)

El eMRTD PUEDE ofrecer un UID/PUPI aleatorio o fijo, tal como se define en [ISO/IEC 14443-3].

Se RECOMIENDA utilizar un UID/PUPI aleatorio para mejorar la privacidad del titular del eMRTD y reducir la posibilidad de seguimiento.

B.9 GAMA DE FRECUENCIAS DE RESONANCIA (RECOMENDADO)

No existen requisitos sobre la frecuencia de resonancia. Quienes soliciten un eMRTD PUEDEN limitar la frecuencia de resonancia por defecto a una gama de valores dada a fin de aumentar la interoperabilidad.

B.10 TAMAÑOS DE TRAMA (RECOMENDADO)

El eMRTD PUEDE admitir tamaños de trama de hasta 4 kbyte con arreglo a [ISO/IEC 14443]. No obstante, se RECOMIENDA admitir tamaños de trama de al menos 1 kbyte. Si se admiten tamaños de trama superiores a 1 kbyte, se RECOMIENDA utilizar tramas con la corrección de errores definida en [ISO/IEC 14443-4].

Nota.— Un tamaño de trama superior reduce sustancialmente el tiempo total de procesamiento de una aplicación del eMRTD.

B.11 ENTERO CORRESPONDIENTE AL TIEMPO DE ESPERA DE TRAMA (FWI) Y PETICIÓN DE PRÓRROGA DEL TIEMPO DE ESPERA DEL BLOQUE-S [S(WTX)] (RECOMENDADO)

Se RECOMIENDA que se fije un valor de FWI para el eMRTD menor o igual a 11 para mejorar la calidad de funcionamiento. Se RECOMIENDA utilizar instrucciones S(WTX) para ampliar el tiempo de espera de trama para cada instrucción que requiera tiempo adicional mediante el uso de instrucciones S(WTX) con un WTXM no superior a 10.

Si se envían varias solicitudes S(WTX) al eMRTD, se RECOMIENDA que el tiempo de procesado total para el bloque I-Block no supere los 5 s.

Nota.— Valores inferiores de FWI tal como se RECOMIENDA aquí disminuyen sustancialmente la pérdida de tiempo debida a errores de transmisión, mientras que las S(WTX) son el medio ideal para proporcionar más tiempo cuando sea necesario.

— — — — — — — —

Apéndice C de la Parte 10

SISTEMAS DE INSPECCIÓN (INFORMATIVO)

C.1 VOLUMEN OPERACIONAL Y POSICIONES EN LOS ENSAYOS

Un sistema de inspección asociado al eMRTD tendrá un volumen operacional conforme a uno de los tipos de sistema de inspección definidos en [ISO/IEC 18745-2]. El volumen operacional es el volumen para el que se satisfacen todos los requisitos del presente informe técnico.

Nota.— Las posiciones de ensayo para cada tipo de sistema de inspección se especifican con más detalle en [ISO/IEC 18745-2] con respecto a la superficie (del dispositivo) de 0 mm del sistema de inspección asociado al eMRTD.

C.2 FORMA DE ONDA ESPECÍFICA Y REQUISITOS DE RF

Las formas de onda del campo magnético alterno utilizado para la comunicación serán plenamente conformes con [ISO/IEC 14443-2]. En general, no hay excepciones o divergencias con respecto a la norma básica, excepto en lo referente a la intensidad de campo.

Para los sistemas de inspección asociados al eMRTD de **Tipo 1, 2 y 3**, se RECOMIENDA que la intensidad de campo sea de al menos dos A/m en todas las posiciones para la clase 1. Para los sistemas de inspección asociados al eMRTD de Tipo M, la intensidad de campo será de al menos 1,5 A/m en todas las posiciones para la clase 1.

Nota.— Puede ser conveniente que el eMRTD también se comunique con otros sistemas de inspección sin contacto y con dispositivos móviles. Por ejemplo, los teléfonos inteligentes con NFC utilizan 1,5 A/m.

C.3 SECUENCIAS DE INTERROGACIÓN Y TIEMPO DE DETECCIÓN DEL eMRTD

La secuencia de interrogación del sistema de inspección asociado al eMRTD proporcionará 10 ms de portadora no modulada antes de cualquier REQA/WUPA o REQB/WUPB.

Para una detección y procesamiento rápidos, el sistema de inspección del eMRTD:

- sondeará en busca del Tipo A y del Tipo B con el mismo número de peticiones para ambos tipos;
- para los sistemas de inspección de Tipos 1, 2 y 3 debería producirse un reinicio de RF entre cualquier REQ/WUP del mismo tipo
- garantizará al menos una instrucción de interrogación para el Tipo A y el Tipo B, en un plazo de 150 ms para un eMRTD presente en el volumen operacional obligatorio mínimo con arreglo a [ISO/IEC 18745-2] en cualquier posición.

El sistema de inspección del eMRTD PUEDE interrogar en busca de productos son contacto con cualquier otro tipo de modulación sobre la portadora de 13,56 MHz, siempre que se cumplan los requisitos arriba indicados.

Nota.— La portadora no modulada de 10 ms es necesaria para detectar todos los eMRTD existentes en el entorno, basada en especificaciones anteriores.

C.4 VELOCIDADES BINARIAS OBLIGATORIAS

El sistema de inspección asociado al eMRTD proporcionará con carácter obligatorio: 106 kbit/s y 424 kbit/s en ambos sentidos desde el eMRTD hasta el sistema de inspección asociado al eMRTD y viceversa.

La velocidad binaria de 212 kbit/s, y todas las velocidades binarias desde 848 kbit/s hasta 6,78 Mbit/s en ambos sentidos, y de 10,17 Mbit/s a 27.12 Mbit/s desde el sistema de inspección del eMRTD al eMRTD, tal como se define en [ISO/IEC 14443-2], son opcionales.

C.5 PERTURBACIÓN ELECTROMAGNÉTICA (EMD)

No es obligatorio admitir la EMD.

Nota.— El hecho de soportar la EMD mejora la robustez de la comunicación sin contacto entre el eMRTD y el sistema de inspección asociado al eMRTD contra la perturbación electromagnética generada por el eMRTD. El consumo dinámico de corriente del eMRTD durante la ejecución de una instrucción puede tener un efecto aleatorio de modulación de la carga (que puede no ser completamente resistiva) sobre el campo magnético. En algunos casos, el sistema de inspección asociado al eMRTD puede interpretar erróneamente la EMD como datos enviados por el eMRTD, lo que puede afectar negativamente a la correcta recepción de la respuesta del eMRTD.

C.6 CLASES DE ANTENAS ADMITIDAS

El sistema de inspección asociado al eMRTD de **Tipo 1** y de **Tipo 2** admitirá al menos los eMRTD de clase 1 en el volumen operacional.

La Clase 2 y la Clase 3 son obligatorias en ISO/IEC 14443, pero son opcionales para el sistema de inspección del eMRTD.

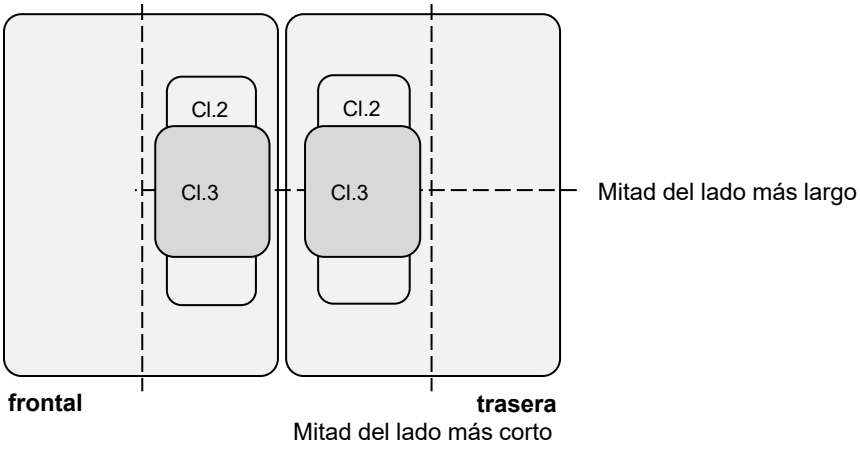


Figura C-1. Posiciones obligatorias en cada superficie de ID-3 en la que un sistema de inspección asociado a un eMRTD de tipo 1 y 2 leerá las antenas de clase 2 y 3

C.7 TAMAÑOS DE TRAMA Y CORRECCIÓN DE ERRORES (OPCIONAL)

El sistema de inspección asociado al eMRTD PUEDE soportar opcionalmente todos los tamaños de trama de hasta 4 kbytes tal como se define en [ISO/IEC 14443-3]. Se RECOMIENDA utilizar tramas con corrección de errores tal como se define en [ISO/IEC 14443-3] para todos los tamaños de trama soportados de más de 1 kbyte.

Nota.— Para sistemas de inspección de tipo M asociados al eMRTD, actualmente no se prevé que existan tamaños de trama superiores a 256 bytes.

C.8 ADMISIÓN DE CLASES ADICIONALES (OPCIONAL)

Los sistemas de inspección asociados al eMRTD de todos los tipos PUEDEN soportar además las Clases 4, 5 y 6 para el interfuncionamiento, por ejemplo, con dispositivos móviles, lo que produce un menor acoplamiento con el bobinado de la antena del sistema de inspección asociado al eMRTD.

C.9 TEMPERATURA OPERACIONAL (RECOMENDADO)

Se RECOMIENDA que el sistema de inspección asociado al eMRTD pueda operar en un rango de temperatura entre –10° y 50° Celsius.

C.10 ADMISIÓN DE eMRTD MÚLTIPLES Y OTRAS TARJETAS, OBJETOS O ANFITRIONES MÚLTIPLES (RECOMENDADO)

Se RECOMIENDA encarecidamente diseñar el sistema de inspección asociado al eMRTD para que gestiones más de un eMRTD o bien un eMRTD y otra tarjeta u objeto conforme con [ISO/IEC 14443].

PUEDE aplicarse una de las reglas o combinaciones siguientes:

- Aplicar algoritmos completos anticolisión definidos en [ISO/IEC 14443-3],
- Verificar el soporte de [ISO/IEC 14443-4] y descartar todas las tarjetas que no lo soportan,
- Verificar que existe una aplicación del eMRTD,
- Utilizar identificador de tarjeta (CID) y dirección de nodo (NAD).

Nota.— También puede utilizarse NAD para dispositivos móviles con varios anfitriones.

C.11 TAMAÑOS DE TRAMA (RECOMENDADO)

El sistema de inspección asociado al eMRTD PUEDE soportar tamaños de trama de hasta 4 kbytes conforme a [ISO/IEC 14443-3]. No obstante, se RECOMIENDA soportar tamaños de trama de al menos 1 kbyte. Si se soportan tamaños de trama de 1 kbyte o mayores, se RECOMIENDA el uso de tramas con corrección de errores tal como se define en [ISO/IEC 14443-4].

Se RECOMIENDA realizar la división de la carga útil de la capa de aplicación en un número mínimo de tramas con una longitud efectiva correspondiente al tamaño de trama máximo soportado con la excepción de la última trama.

C.12 RECUPERACIÓN DE ERRORES (RECOMENDADO)

Posteriormente a un error de transmisión o a un eMRTD que no responda, se RECOMIENDA que el sistema de inspección asociado al eMRTD envíe un segundo bloque-R que contenga un reconocimiento negativo R(NAK) conforme a la regla 4 del sistema de inspección de [ISO/IEC 14443-4].

C.13 DETECCIÓN DE ERRORES Y MECANISMO DE RECUPERACIÓN (RECOMENDADO)

Si cuando se utilicen velocidades binarias opcionales así como tamaños de tramas opcionales superiores a 256 bytes, se produce un número superior al habitual de errores de transmisión, se RECOMIENDA reducir la velocidad binaria y el tamaño de trama efectivo.

— — — — — — — —

Apéndice D de la Parte 10

OBJETO DE SEGURIDAD DEL DOCUMENTO EF.SOD VERSIÓN V0 PARA LA LDS V1.7 (VERSIÓN ANTERIOR) (INFORMATIVO)

El objeto de seguridad del documento V0 para la LDS v1.7 no contiene la información sobre la versión de la LDS y la versión Unicode:

```
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash}
```

D.1 TIPO DE DATOS FIRMADOS PARA SO_D V0

El objeto de seguridad del documento se implementa como tipo de datos firmados (SignedData), según se especifica en [RFC 3369]. Todos los objetos de seguridad SE PRODUCIRÁN en formato de regla de codificación distinguida (DER) para preservar la integridad de las firmas que contengan.

Nota 1.— m = OBLIGATORIO — el campo ESTARÁ presente.

Nota 2.— x = no utilizar — el campo NO DEBERÍA llenarse.

Nota 3.— o = opcional — el campo PUEDE estar presente.

Nota 4.— c = elección — el contenido del campo es una elección entre varias alternativas.

Tabla D-1. Tipo de datos firmados para SO_D V0

Valor		Comentario
SignedData		
Version	m	Valor = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-mrtd-security-ldsSecurityObject
eContent	m	El contenido codificado de un ldsSecurityObject.
Certificates	o	Los Estados pueden optar por incluir el certificado de firmante del documento (C_{DS}), que puede utilizarse para verificar la firma en el campo signerInfos.
Crls	x	Se recomienda que los Estados no utilicen este campo.
signerInfos	m	Se recomienda que los Estados solo proporcionen 1 signerInfo en este campo.
SignerInfo	m	
Version	m	El valor de este campo está dictado por el campo sid. Véanse las reglas relativas a este campo en RFC3369, Doc 9303-12.
Sid	m	
issuerandSerialNumber	c	Se recomienda que los Estados admitan este campo en lugar de subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	El identificador del algoritmo utilizado para producir el valor condensado sobre encapsulatedContent y SignedAttrs.
signedAttrs	m	Los Estados productores quizás deseen incluir atributos adicionales para incorporarlos a la firma; no obstante, estos no tienen que ser procesados por los Estados receptores, excepto para verificar el valor de la firma.
signatureAlgorithm	m	El identificador del algoritmo utilizado para producir el valor de la firma y cualquier otro parámetro conexo.
Signature	m	El resultado del proceso de generación de firma.
unsignedAttrs	o	Los Estados productores quizás deseen utilizar este campo, pero no se recomienda y los Estados receptores pueden optar por hacer caso omiso del mismo.

D.2 Objeto de seguridad deL documento de LA LDS DEL perfil ASN.1 PARA SO_D V0

```
LDSSecurityObjectV0 {joint-iso-itu-t (2) international(23) icao(136) mrtd(1)
security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS

-- Importaciones de RFC 3280 [PERFIL],
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) };

-- Constantes

ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao   OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}
id-icao-mrtd  OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security     OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 1}

-- Objeto de seguridad LDS

LDSSecurityObjectVersion ::= INTEGER {v0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber        DataGroupNumber,
   dataGroupHashValue     OCTET STRING }
DataGroupNumber ::= INTEGER {
   dataGroup1        (1),
   dataGroup2        (2),
   dataGroup3        (3),
   dataGroup4        (4),
   dataGroup5        (5),
   dataGroup6        (6),
   dataGroup7        (7),
   dataGroup8        (8),
   dataGroup9        (9),
   dataGroup10             (10),
   dataGroup11             (11),
   dataGroup12             (12),
   dataGroup13             (13),
   dataGroup14             (14),
   dataGroup15             (15),
   dataGroup16             (16)}
END
```

Nota 1.— El campo `dataGroupHashValue` *contiene la condensación calculada del contenido completo del EF de grupo de datos, especificado por* `dataGroupNumber`*.*

Nota 2.— Los `DigestAlgorithmIdentifiers` *DEBEN omitir los parámetros* `NULL`*, mientras que el* `SignatureAlgorithmIdentifier` *definido en RFC 3447) DEBE incluir* `NULL` *como parámetro si no hay parámetros presentes, incluso cuando se usen algoritmos SHA2 con arreglo a RFC 5754. El sistema de inspección DEBE aceptar el campo* `DigestAlgorithmIdentifiers` *con ambas condiciones, es decir, parámetros ausentes y parámetros* `NULL`*.*

— — — — — — — —

Apéndice E de la Parte 10

RESUMEN DE LA ESTRUCTURA DE FICHERO (INFORMATIVO)

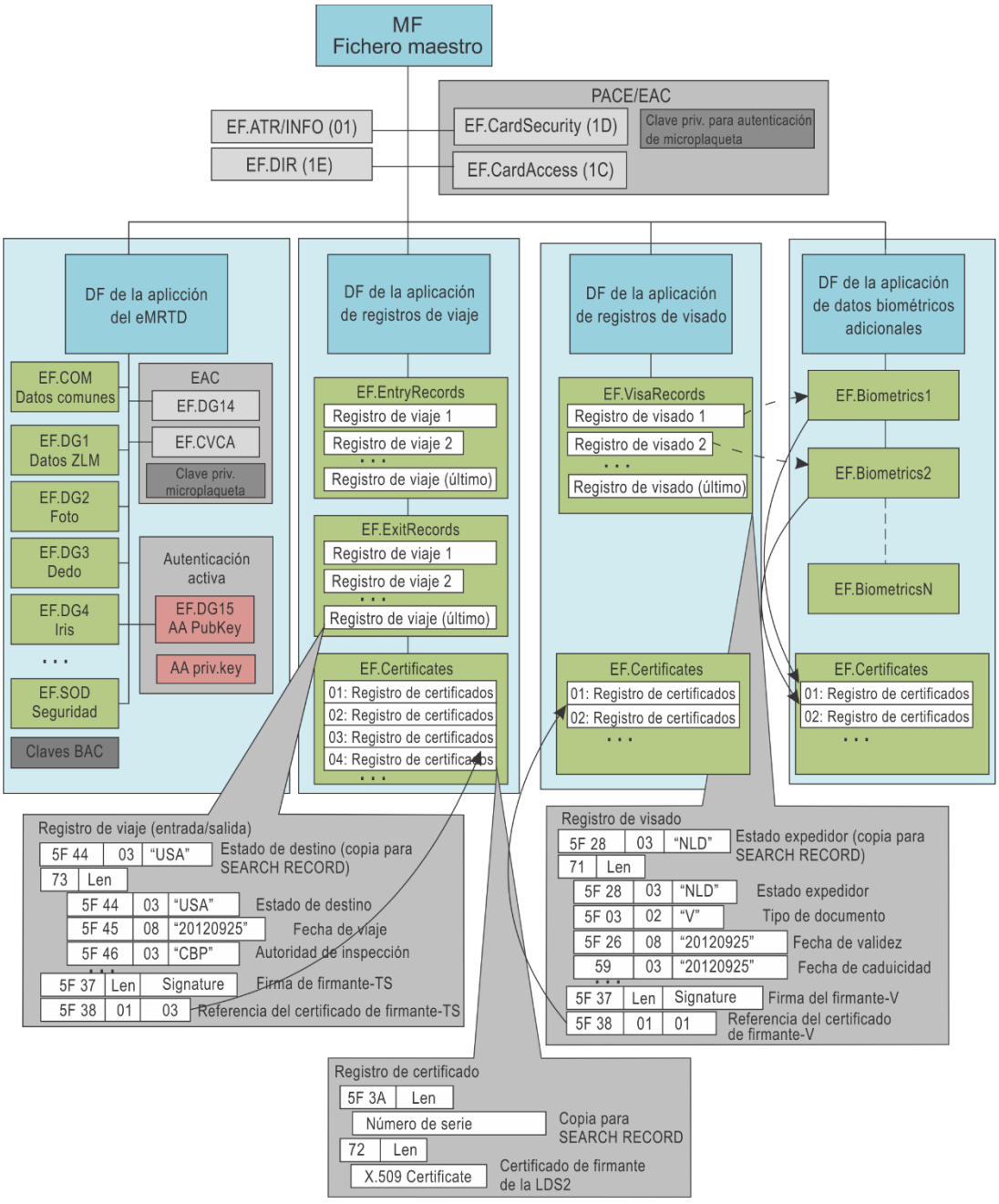


Figura E-1. Resumen de las estructuras de fichero

— — — — — — — —

Apéndice F de la Parte 10

RESUMEN DE LA AUTORIZACIÓN DE LA LDS
(INFORMATIVO)

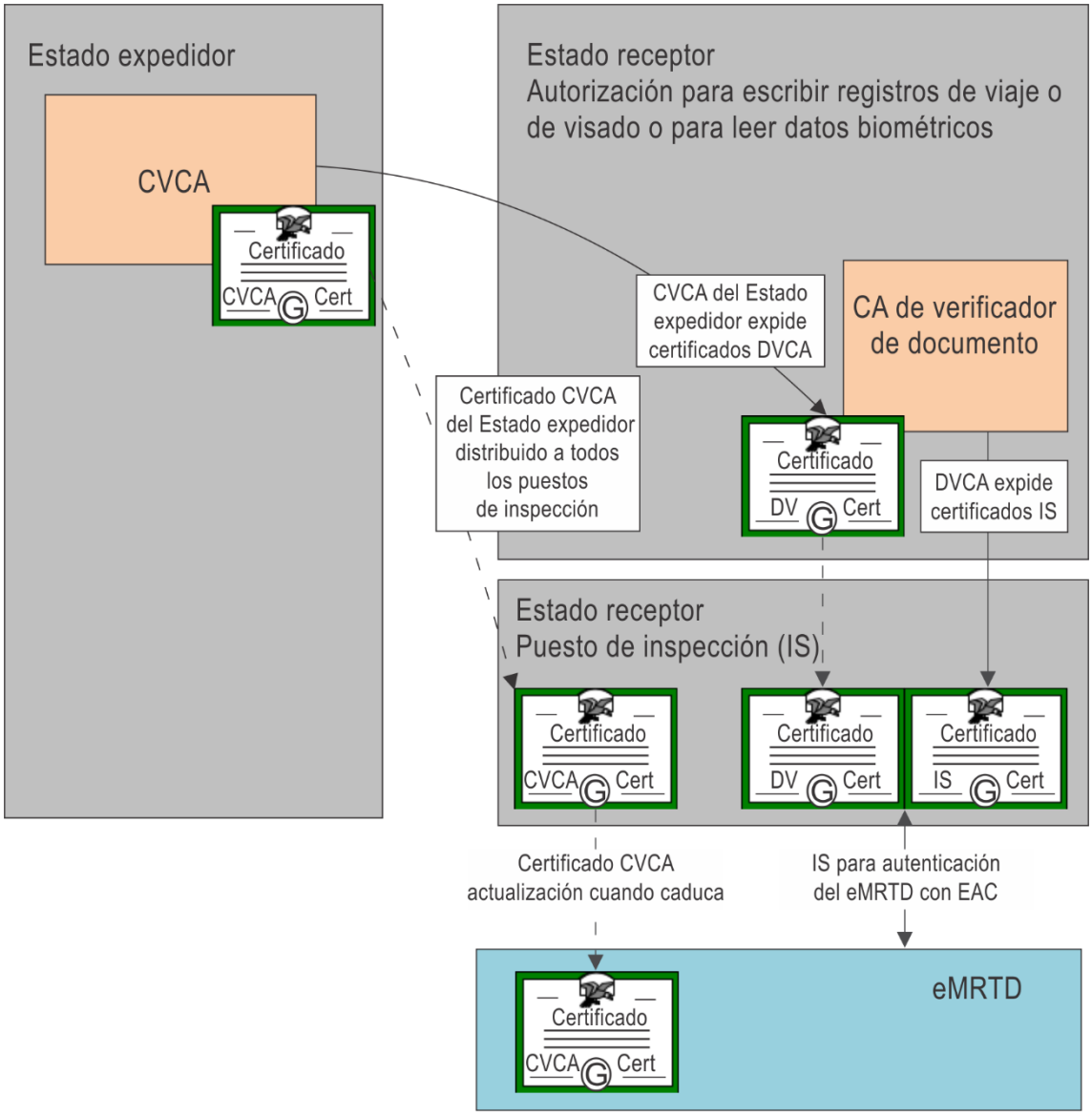


Figura F-1. Resumen de la autorización de la LDS

— — — — — — — —

Apéndice G de la Parte 10

RESUMEN DE LA FIRMA DIGITAL DE LA LDS
(INFORMATIVO)

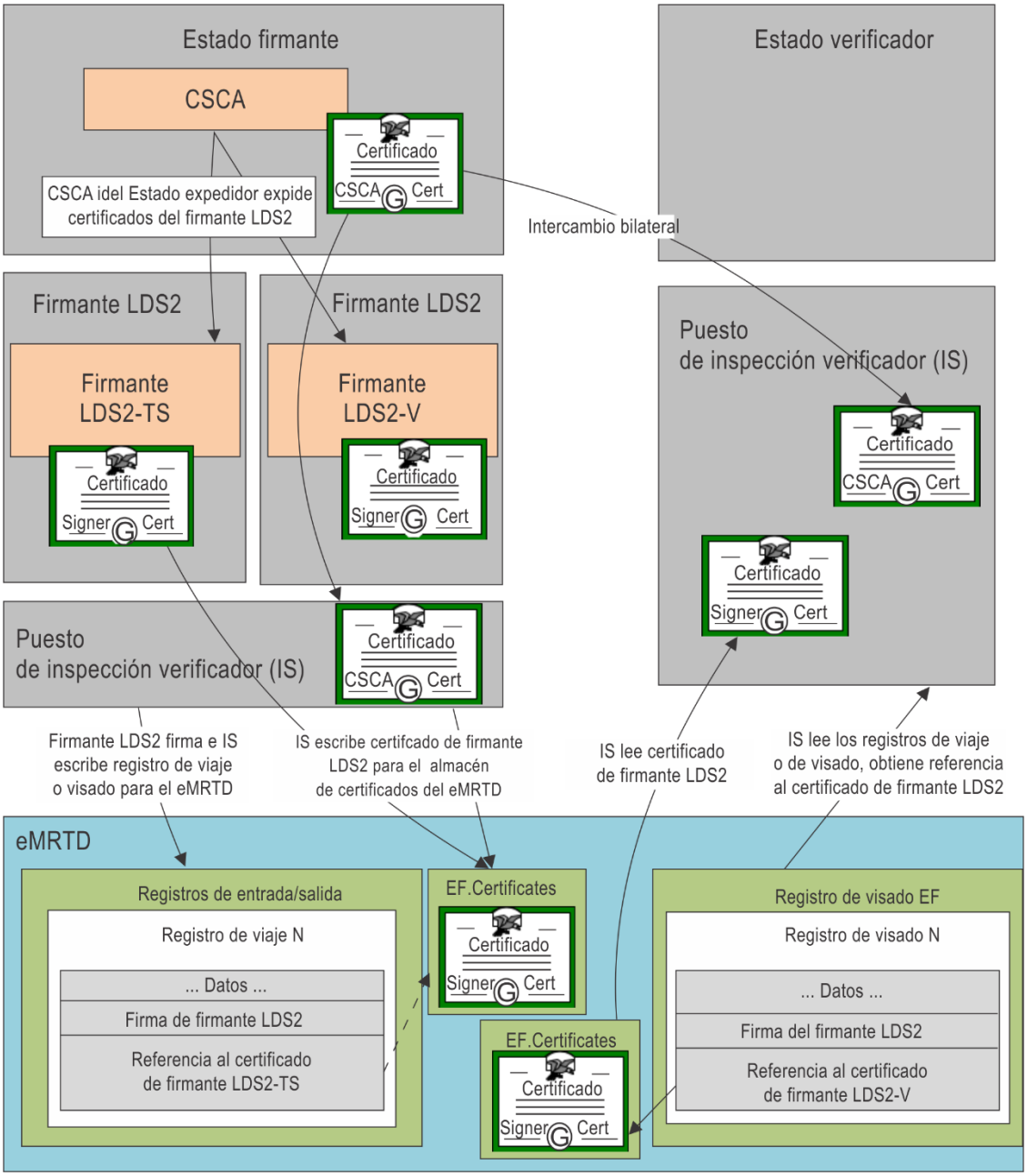


Figura G-1. Firma digital de la LDS

— — — — — — — —

Apéndice H de la Parte 10

EJEMPLO DE LECTURA DE REGISTRO DE VIAJE (INFORMATIVO)

H.1 COMANDO FMM PARA LA RECUPERACIÓN DEL NÚMERO DE REGISTROS DE ENTRADA

CLA	INS	P1	P2	Lc	Datos	Le
'80'	'5E'	'01'	'04'	'04'	'51 02 01 01'	'00'

CLA: Clase propia / no hay mensajería segura
INS: FMM
P1: '01' —Identificador EF del campo de datos de comando
P2: '04' — Devolución del número existente de registros en un EF de registro
Lc: '04'
Data: DO'51' — contiene el identificador del EF de registros de entrada '0101'
Le: '00' (Le breve)

Respuesta: El DO FILE AND MEMORY MANAGEMENT representa el número de registros contenidos en el EF.

Datos	SW1-SW2
'7F78 03' '83 01 FD'	'90 00'

El DO de los datos de respuesta contiene el último número de registro que puede utilizarse en el siguiente comando READ RECORD (P1).

Por ejemplo, el último número de registro '00' significa que no hay registros en este archivo y la respuesta 'FD' significa que el número de registros es de 253 (el número máximo de registros es de 254).

H.2 COMANDO READ RECORD PARA LA RECUPERACIÓN DEL ÚLTIMO REGISTRO DE VIAJE DE LA LISTA RECUPERADA

El siguiente comando puede usarse para recuperar un registro individual utilizando el número de registro devuelto por el comando FMM:

CLA	INS	P1	P2	Le
'00'	'B2'	'FD'	'04'	'00 00 00'

CLA: Clase interindustrial / no hay mensajería segura
INS: READ RECORD(S)
P1: Número de registro de la respuesta del comando anterior
P2: Número de registros en P1 / Leer registros P1
Le: '00 00 00' (Le ampliado), leer el registro entero

Respuesta: El número de registro es 253 ('FD').

Datos	SW1-SW2
'5F44' 'Len' <Data> || '73' 'Len' <Data> || '5F37' 'Len' <Data> || '5F38' 'Len' <Data>	'90 00'

H.3 COMANDO READ RECORD PARA LA RECUPERACIÓN DE LOS DOS ÚLTIMOS REGISTROS DE VIAJE DE LA LISTA RECUPERADA

El siguiente comando puede usarse para recuperar dos (o más) registros de la lista devuelta por el comando FMM. La lectura de varios registros del intercambio de una APDU mejora el rendimiento. El número de registros que puede recuperar un solo comando puede determinarse a partir de la información de longitud ampliada en EF.ATR/INFO y el tamaño máximo del registro de viaje.

CLA	INS	P1	P2	Le
'00'	'B2'	'FC'	'05'	'00 00 00'

CLA: Clase interindustrial / no hay mensajería segura
INS: READ RECORD(S)
P1: Número de registro disminuido de la respuesta FMM (253 - 1 = 252 = 'FC')
P2: Número de registros en P1 / Leer todos los registros desde P1 hasta el último registro
Le: '00 00 00' (Le ampliado), leer el registro entero

Respuesta: Se devuelven los dos últimos registros: 252 ('FC') y 253 ('FD').

Datos	SW1-SW2
'5F44' 'Len' <Data> || '73' 'Len' <Data> || '5F37' 'Len' <Data> || '5F38' 'Len' <Data> || '5F44' 'Len' <Data> || '73' 'Len' <Data> || '5F37' 'Len' <Data> || '5F38' 'Len' <Data>	'90 00'

— — — — — — — —

Apéndice I de la Parte 10

EJEMPLO DE BÚSQUEDA DE REGISTROS POR UN ESTADO (INFORMATIVO)

I.1 BÚSQUEDA CON EL COMANDO SEARCH RECORD EN REGISTRO(S) DE VIAJE POR EL ESTADO DE DESTINO

CLA	INS	P1	P2	Lc	Datos	Le
'00'	'A2'	'00'	'F8'	Var	'7F 76' 'Len' '51 01 01' 'A1 0B' '80 01 00' 'B0 06' '02 01 03' '02 01 03' 'A3 07' 'B1 05' '81 03' xx xx xx	'00'

CLA: Clase interindustrial / no hay mensajería segura
INS: SEARCH RECORD(S)
P1: Número de registro = '00'
P2: Búsqueda en múltiples EF
Lc: Longitud del campo de datos de comando
Datos: DO'7F76' – DO Gestión de registros
DO'51' - DO Referencia de fichero (Identificador EF.EntryRecords breve '01')
DO'A1' - Búsqueda en plantilla de configuración
DO'80' - Búsqueda en parámetro de configuración: '00' (búsqueda en todos los registros)
DO'B0' - Plantilla de la ventana de búsqueda
DO'02' - Desplazamiento: '03'
DO'02' – Número de bytes: '03'
DO'A3' - Búsqueda en la plantilla de cadena
DO'B1' – DO Búsqueda en la cadena
DO'81' - Búsqueda en la cadena (código del país): xx xx xx
Le: '00' (Le breve)

Respuesta: DO'7F76' –DO Gestión de registros
DO'51' - Identificador EF.EntryRecords breve '01'
Uno o más DO'02' que contienen los números de registro correspondientes

Datos	SW1-SW2
‘7F 76’ ‘Len’’ ‘51 01 01’ ‘02 01 03’ ‘02 01 04’	‘90 00’

— — — — — — — —

Apéndice J de la Parte 10

EJEMPLO DE ESCRITURA DE REGISTRO DE VIAJE Y CERTIFICADO (INFORMATIVO)

J.1 BÚSQUEDA CON EL COMANDO SEARCH RECORD EN EF.CERTIFICATES POR NÚMERO DE SERIE DEL CERTIFICADO

El IS comprueba si el certificado del firmante de la LDS2-TS con los números de serie requeridos existe en EF.Certificates. Puede usarse el siguiente comando para buscar en los certificados:

CLA	INS	P1	P2	Lc	Datos	Le
'00'	'A2'	'00'	'F8'	Var	'7F 76' 'Len' '51 01 1A' 'A1 0B' '80 01 30' 'B0 06' '02 01 03' '02 01' { Búsqueda en los bytes de la cadena} 'A3' 'Len' 'B1' 'Len' '81' 'Len' xx xx .. xx xx	'00'

CLA: Clase interindustrial / no hay mensajería segura INS: SEARCH RECORD(S)
P1: Número de registro = '00'
P2: Búsqueda en múltiples EF
Lc: Longitud del campo de datos de comando
Data: DO'7F76' – DO Gestión de registros
DO'51' - DO Referencia de fichero (Identificador EF.Certificates breve '1A') DO'A1' - Búsqueda en plantilla de configuración
DO'80' - Búsqueda en parámetro de configuración: '30' (interrupción si se encuentra el registro)
DO'B0' - Plantilla de la ventana de búsqueda
DO'02' - Desplazamiento: '03'
DO'02' – Número de bytes: Búsqueda en los bytes de la cadena
DO'A3' - Búsqueda en la plantilla de cadena
DO'B1' – DO Búsqueda en la cadena
DO'81' – Búsqueda en concatenación de código del país y número de serie del certificado: xx xx .. xx xx
Le: '00' (Le breve)

Respuesta: DO'7F76' – DO Gestión de registros
DO'51' - Identificador EF.Certificates breve '1A'
DO'02' – contiene el número de registro correspondiente

Datos	SW1-SW2
'7F 76 06' '51 01 1A' '02 01 01'	'90 00'

o código de aviso '62 82' si ningún registro se corresponde con los criterios de búsqueda:

SW1-SW2
'62 82'

Si un registro EF.Certificate se corresponde con los criterios de búsqueda, opcionalmente el IS puede utilizar el número de registro devuelto ('01') en un comando READ RECORD para comprobar si el certificado es el correcto. Si ningún registro EF.Certificate se corresponde con los criterios de búsqueda, el IS escribe el certificado en EF.Certificates utilizando el comando APPEND RECORD de la sección J.2 y, por último, escribe el registro de entrada usando el comando APPEND RECORD en la sección J.3.

J.2 COMANDO APPEND RECORD para escribir CERTIFICADO

El IS escribe el certificado de firmante de la LDS2-TS en EF.Certificates. Puede usarse el siguiente comando para escribir en los certificados:

CLA	INS	P1	P2	Lc	Data	Le
'00'	'E2'	'00'	'D0'	'00' XX XX	'5F3A' 'Len' {número de serie del certificado} || '72' 'Len' {certificado X.509 }'	Ausente

CLA: Clase interindustrial / no hay mensajería segura
INS: APPEND RECORD
P1: '00' (ningún otro valor es válido)
P2: Identificador EF breve (= '1A')
Lc: Longitud del registro (Lc ampliado)
Datos: Datos del registro

Respuesta: Código de éxito o de error

SW1-SW2
'90 00'

J.3 COMANDO APPEND RECORD PARA ESCRIBIR REGISTRO DE VIAJE

El IS genera un registro de viaje usando la referencia al certificado de firmante de la LDS2-TS y lo escribe en EF.EntryRecords utilizando el siguiente comando:

CLA	INS	P1	P2	Lc	Datos	Le
'00'	'E2'	'00'	'08'	'00' XX XX	'5F44' 'Len' {Estado de destino} || '73' 'Len' {Registro de viaje de entrada} || '5F37' 'Len' {Firma} || '5F38' 'Len' {Ref Cert}	Ausente

CLA: Clase interindustrial / no hay mensajería segura
INS: APPEND RECORD
P1: '00' (ningún otro valor es válido)
P2: Identificador EF breve (= '01')
Lc: Longitud del registro (Lc ampliado)
Data: Datos del registro

Respuesta: Código de éxito o de error

SW1-SW2
'90 00'

— FIN —

ISBN 978-92-9265-559-4