OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Parte 9: Empleo de identificación biométrica y almacenamiento electrónico de datos en los MRTD

Aprobado 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

Parte 9: Empleo de identificación biométrica y almacenamiento electrónico de datos en los MRTD

Aprobado 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, Montréal, Québec, Canada H3C 5H7

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

Doc 9303, *Documentos de viaje de lectura mecánica*
Parte 9 — *Empleo de identificación biométrica y almacenamiento electrónico de datos en los MRTD*
Pedido Num.: 9303P9
ISBN 978-92-9265-485-6 (versión impresa)
ISBN 978-92-9275-343-6 (versión electrónica)

ENMIENDAS

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de productos y servicios* de la OACI; 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 CORRIGENDA

ENMIENDAS		
Núm.	Fecha	Anotada por
1	20/3/24	OACI

CORRIGENDA			
Núm.	Fecha	Idioma	Anotada por

ÍNDICE

1. ALCANCE

En la Parte 9 del Doc 9303 se definen las especificaciones, adicionales a las presentadas para el MRTD básico en las Partes 3, 4, 5, 6 y 7 del Doc 9303, que han de aplicar los Estados u organizaciones que deseen expedir un documento oficial de viaje de lectura mecánica electrónico (eMRTD) que pueda utilizarse por cualquier Estado receptor u organización receptora debidamente equipados para leer y autenticar datos relativos al propio eMRTD y a la verificación de su titular. Esto comprende datos biométricos obligatorios de interfuncionamiento mundial que puedan utilizarse como entradas para los sistemas de reconocimiento de rostro y, como opción, a los sistemas de reconocimiento de huellas digitales o del iris. Las especificaciones exigen que los datos biométricos de interfuncionamiento mundial se almacenen en forma de imágenes de alta resolución en un circuito integrado (CI) sin contacto, de elevada capacidad, también codificado con un duplicado de los datos de la ZLM. Las especificaciones también permiten el almacenamiento de una gama de datos opcionales a discreción del Estado expedidor o de la organización expedidora. Dado que el uso del circuito integrado sin contacto es independiente del tamaño del documento, todas las especificaciones se aplican a todos los tamaños eMRTD en su forma electrónica. Las diferencias entre los formatos del eMRTD se relacionan con la ZLM, con consecuencias para el almacenamiento de la ZLM en el CI sin contacto. Dichas diferencias se indican en las especificaciones de la estructura lógica de datos en el Doc 9303-10.

La Parte 9 deberá leerse conjuntamente con:

- Parte 1 — *Introducción*;
- Parte 10 — *Estructura lógica de datos (LDS) para el almacenamiento de datos biométricos y de otro tipo en el circuito integrado (CI) sin contacto*;
- Parte 11 — *Mecanismos de seguridad para los MRTD*;
- Parte 12 — *Infraestructura de clave pública para los MRTD*.

2. eMRTD

Nota.— Los términos MRTD y eMRTD se utilizan en este documento como referencia genérica a todos los tipos de documentos de viaje de lectura mecánica en, respectivamente, formato de lectura de caracteres ópticos y formato electrónico. Los términos DV1, DV2 y DV3 se refieren a los diferentes formatos de MRTD. Todos los eMRTD a que se hace referencia en esta parte son electrónicos.

2.1 Cumplimiento de las especificaciones del Doc 9303

Un MRTD electrónico (eMRTD) SE AJUSTARÁ totalmente a las especificaciones proporcionadas en el Doc 9303.

2.2 Período de validez del eMRTD

El período de validez del eMRTD queda a discreción del Estado expedidor o de la organización expedidora; no obstante, considerando la duración limitada de los documentos y los cambios de aspecto de la persona titular del documento con el tiempo, se RECOMIENDA un período de validez que no supere los diez años. PUEDE considerarse un período más breve para permitir la actualización progresiva del eMRTD a medida que evoluciona la tecnología.

2.3 Símbolo de microplaqueta contenida

La Parte 9 del Doc 9303-9 se concentra en los aspectos biométricos en relación con los documentos de viaje de lectura mecánica utilizando el término “eMRTD” para denominar a dichos MRTD con capacidad biométrica y de interfuncionamiento mundial. Los MRTD que no se ajusten a las especificaciones del Doc 9303 no pueden denominarse eMRTD y no tendrán el símbolo de microplaqueta contenida.

Todos los eMRTD llevarán el símbolo siguiente:

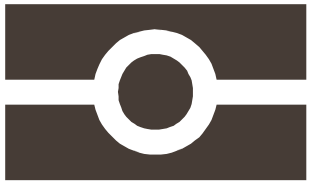


Figura 1. Símbolo de microplaqueta contenida

En el sitio web de la OACI se dispone de un fichero electrónico de este símbolo. El símbolo solo APARECERÁ en un eMRTD que contenga un circuito integrado sin contacto, con capacidad de almacenamiento de datos suficiente para dar cabida a todos los datos obligatorios con arreglo a la estructura lógica de datos (Doc 9303-10), estando todos los datos ingresados protegidos con una firma digital según se especifica en el Doc 9303-11. A menos que un eMRTD se ajuste a estos requisitos mínimos, NO SERÁ catalogado como eMRTD ni presentará el símbolo de microplaqueta contenida. Este símbolo aparecerá en el anverso del eMRTD si se trata de una libreta de tamaño DV3 (eMRP) ya sea cerca de la parte superior o inferior de la cubierta o en el anverso del eMRTD, si se trata de una tarjeta (eMROTD).

En el eMRP el símbolo se incluirá en el entramado u otra imagen estampada en la cubierta exterior. Se recomienda que el símbolo también se estampe en la página de datos en un color adecuado y en un lugar que no interfiera con la lectura de otros datos. El Estado expedidor u organización expedidora también puede estampar el símbolo en la página interior o cubierta de la libreta del pasaporte que contenga el CI sin contacto y, a su discreción, en cualquier otro lugar del pasaporte.

En el eMROTD el símbolo APARECERÁ en el anverso del documento preferentemente en la Zona I.

La imagen, como se muestra en la Figura 1, es positiva, es decir la parte negra de la imagen se imprimirá o se representará de otra forma. Se RECOMIENDA que el símbolo aparezca en forma visible al ojo y sea fácilmente reconocible.

En la Figura 2 se muestran las dimensiones RECOMENDADAS del símbolo tal como deben aparecer en la cubierta o página de datos del eMRP o en un DV2 electrónico.

Se RECOMIENDA un tamaño menor de 4,2 × 7,2 mm (0,17 × 0,28 in), proporcionado a escala, para utilizar en un DV1 electrónico.

El símbolo PUEDE proporcionarse a escala para utilizar, por ejemplo, en diseños de fondo.

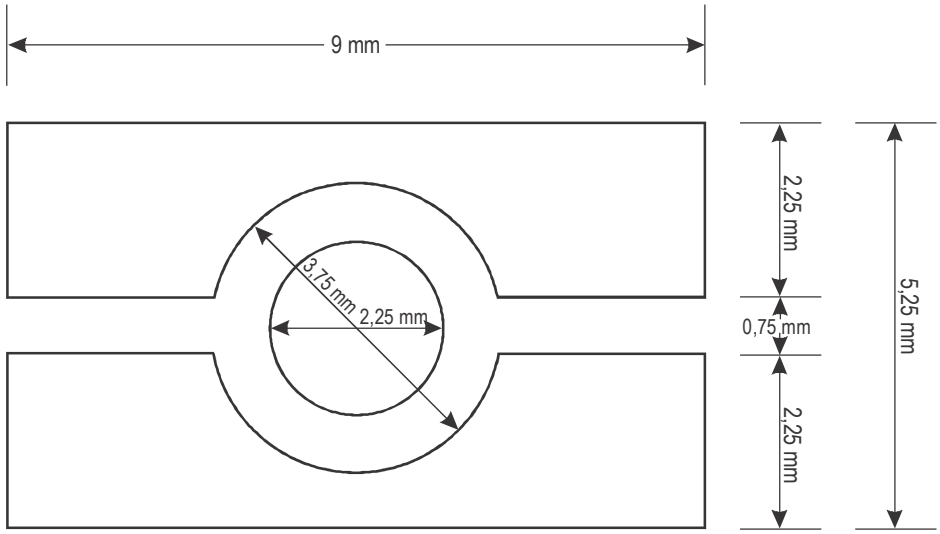


Figura 2. Dimensiones del símbolo

Nota.— Las siguientes son las dimensiones correspondientes en pulgadas: 9,0 mm (0,35 pulgadas), 5,25 mm (0,21 pulgadas), 3,75 mm (0,15 pulgadas), 2,25 mm (0,09 pulgadas), 0,75 mm (0,03 pulgadas).

2.4 Advertencia sobre cuidado en la manipulación de un eMRP

Se sugiere colocar en un lugar obvio de la libreta una advertencia que exhorte a la persona titular de un eMRP a tener el debido cuidado del documento. Se sugiere la redacción siguiente:

“Este pasaporte contiene un dispositivo electrónico sensible. No doble, perfore o exponga el documento a temperaturas extremas o humedad excesiva”.

Además, el Estado expedidor u organización expedidora puede colocar en la parte de la página que contenga el CI y partes correspondientes de algunas páginas vecinas la advertencia:

“No estampe aquí”.

3. IDENTIFICACIÓN BIOMÉTRICA

“Identificación biométrica” es un término genérico utilizado para describir medios automáticos de reconocer una persona viviente mediante la medición de rasgos fisiológicos o de comportamiento distintos.

Una “plantilla biométrica” es una representación codificada a máquina del rasgo en cuestión creada por un algoritmo de soporte lógico de computadora y que permite realizar comparaciones (cotejos) para medir el grado de confianza de que rasgos registrados por separado identifican (o no identifican) a la misma persona. Normalmente, una plantilla biométrica tiene un volumen de datos relativamente pequeño; no obstante, cada fabricante de sistemas biométricos emplea un formato de plantilla propio y las plantillas no son intercambiables entre sistemas. Para permitir que un Estado u organización seleccione el sistema biométrico que se adapte a sus necesidades, los datos deben almacenarse en una forma de la cual su sistema pueda obtener una plantilla. Esto exige que los datos biométricos se almacenen en forma de una o más imágenes.

3.1 Visión de la OACI respecto de la biometría

La visión de la OACI para la aplicación de la tecnología biométrica comprende:

- la especificación de una forma principal interfuncional de la tecnología biométrica para utilizar en el control fronterizo (verificación, listas de vigilancia), así como por los transportistas y expedidores de documentos y la especificación de tecnologías biométricas complementarias convenidas;
- la especificación de las tecnologías biométricas que han de utilizar los expedidores de documentos (identificación, verificación y listas de vigilancia);
- la capacidad de recuperación de datos por un período de 10 años, máxima validez recomendada para un documento de viaje;
- la ausencia de elementos patentados para asegurar que los Estados u organizaciones que invierten en la tecnología biométrica están protegidos contra cambios en la infraestructura o en los proveedores de la misma.

En el Doc 9303 se consideran solamente tres tipos de sistemas de identificación biométrica. Con respecto al almacenamiento de estos tres elementos biométricos en el CI sin contacto de un eMRTD, el Estado expedidor u organización expedidora se AJUSTARÁ a la norma internacional pertinente.

Los tipos de elementos biométricos son:

- reconocimiento del rostro – REQUERIDO
- reconocimiento de huella digital – OPCIONAL;
- reconocimiento del iris – OPCIONAL.

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

- los sistemas de inspección DEBEN poder manejar datos conforme a la ISO/IEC 39794 para el 1/1/2026, después de un período de preparación de seis años a partir del 1/1/2020;
- entre 2026 y 2030, los Estados expedidores u organizaciones expedidoras 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 cuatro años. Durante ese período de transición, serán esenciales las pruebas de interoperabilidad y conformidad;
- del 1/1/2030 en adelante, los Estados expedidores u organizaciones expedidoras DEBERÁN emplear la ISO/IEC 39794-X para la codificación de datos biométricos.

El Doc 9303, Parte 10, Enmienda 1, proporciona orientación acerca de la transición de la ISO/IEC 19794:2005 a la ISO/IEC 39794.

Términos biométricos

Los términos siguientes se emplean en la identificación biométrica:

- “verificar” significa realizar un cotejo de uno a uno entre los datos biométricos ofrecidos obtenidos de la persona titular del eMRTD ahora y una plantilla biométrica creada cuando la persona titular fue inscrita en el sistema;

- "identificar" significa realizar una búsqueda de uno a uno entre los datos biométricos ofrecidos y un conjunto de plantillas que representan a todos los sujetos que han sido inscritos en el sistema.

La biometría puede utilizarse en la función de identificación para mejorar la calidad de la verificación de antecedentes realizada como parte del proceso de solicitud de pasaportes, visados u otros documentos de viaje y pueden utilizarse las características biométricas para establecer un cotejo positivo entre el documento de viaje y la persona que lo presenta.

Para los fines de esta parte, se aplican los términos y definiciones del vocabulario de biometría que figuran en la norma ISO/IEC 2382-37:2017.

3.2 Consideraciones fundamentales

Al especificar las aplicaciones biométricas para eMRTD, las consideraciones fundamentales son:

- *Interfuncionamiento mundial* — la necesidad crucial de especificar un sistema de empleo que se utilice en forma de interfuncionamiento universal;

- *Uniformidad* — la necesidad de minimizar mediante normas específicas, en la medida posible, las diferentes variaciones de solución que podrían introducir los Estados expedidores u organizaciones expedidoras;

- *Fiabilidad técnica* — la necesidad de proporcionar directrices y parámetros para asegurar que los Estados expedidores u organizaciones expedidoras introducen tecnologías que hayan demostrado brindar un elevado nivel de confianza desde el punto de vista de la confirmación de la identidad; y de que los Estados u organizaciones que lean datos codificados por otros Estados expedidores u organizaciones expedidoras puedan asegurarse de que los datos proporcionados son de calidad e integridad suficientes para permitir la verificación exacta en sus propios sistemas;

- *Viabilidad* — la necesidad de asegurar que las normas recomendadas pueden ponerse en práctica e implantarse por los Estados u organizaciones sin que tengan que introducir un conjunto de sistemas y equipos dispares a efectos de ajustarse a todas las posibles variaciones e interpretaciones de las normas;

- *Durabilidad* — el requisito de que los sistemas introducidos funcionarán durante la máxima vida útil recomendada de 10 años de un documento de viaje, y que las actualizaciones futuras serán compatibles retroactivamente.

3.3 Procedimientos fundamentales con respecto a la biometría

Los componentes principales de un sistema biométrico son:

- *Establecimiento de identidad* — seguridad de que la identidad del inscrito se conoce sin dudas;

- *Captación* — adquisición de una muestra biométrica en bruto;

- *Extracción* — conversión de los datos de la muestra biométrica en bruto a una forma intermedia;

- *Creación de plantilla* — conversión de los datos intermedios en plantilla;

- *Comparación* — comparación con la información contenida en una plantilla de referencia almacenada.

Estos procesos involucran:

- El proceso de *inscripción* es la *captura* de una muestra biométrica en bruto. Se utiliza para cada nueva persona (posible titular de eMRTD) de la que se toman muestras de imágenes biométricas para almacenamiento. Este proceso de captación es la adquisición automática de la característica biométrica mediante un dispositivo de captación como un escáner de huellas digitales, un escáner fotográfico, una cámara para imágenes digitales de captación en vivo o una cámara de acercamiento del iris de captación en vivo. Cada dispositivo de captación requerirá ciertos criterios y procedimientos definidos para el proceso de captación — por ejemplo, una pose normalizada enfrentando directamente a la cámara para una captación del reconocimiento del rostro; las huellas digitales se captan en forma plana o por rodamiento; el iris se capta con los ojos completamente abiertos. La imagen resultante se comprime y luego se almacena para futura confirmación de identidad.

- El proceso de *creación de plantillas* conserva las características biométricas distintivas y repetibles de la imagen biométrica captada y en general se efectúa con un algoritmo de soporte lógico patentado para extraer una plantilla de la imagen almacenada. Esto define la imagen en una forma que pueda compararse posteriormente con otra imagen de muestra captada en el momento en que se requiera la confirmación de identidad y una determinada medida de comparación. Inherente a este algoritmo es el control de calidad, por el cual, mediante cierto mecanismo, se establece la calidad de la muestra. Las normas de calidad deben ser lo más elevadas posibles dado que todas las verificaciones futuras dependen de la calidad de la imagen captada originalmente. Si la calidad no es aceptable, el proceso de *captación* debería repetirse.

- El proceso de *identificación* toma la plantilla obtenida de la nueva muestra y la compara con las plantillas almacenadas de los usuarios finales inscritos para determinar si el usuario final ha ingresado en el sistema anteriormente y, de ser así, si lo ha hecho con la misma identidad.

- El proceso de *verificación* toma las nuevas muestras de una persona titular de eMRTD y las compara con una plantilla obtenida de la imagen almacenada de dicho portador para determinar si éste presenta la misma identidad.

3.4 Aplicaciones para una solución biométrica

La aplicación fundamental de una solución biométrica es la verificación de la identidad para relacionar a una persona titular de eMRTD con el eMRTD del que es portador/a.

Existen varias aplicaciones típicas para las características biométricas durante el proceso de inscripción en la solicitud de un eMRTD.

Los datos biométricos del usuario final generados en el proceso de inscripción pueden utilizarse en una búsqueda en una o más bases de datos biométricos (identificación) para determinar si el usuario final es conocido de algunos de los sistemas correspondientes (p. ej., titular de un eMRTD con identidad diferente, antecedentes delictivos, titular de un eMRTD de otro Estado u organización).

Cuando los/as usuarios/as finales recogen el eMRTD (o se presentan para alguna de las etapas del proceso de expedición después de la solicitud inicial y la captación de datos biométricos) sus datos biométricos pueden tomarse nuevamente y verificarse con respecto a los datos biométricos captados inicialmente.

Las identidades del personal encargado de la inscripción pueden verificarse para confirmar que tienen autoridad para realizar las tareas asignadas. Esto puede incluir la autenticación biométrica para iniciar la firma digital de registros de auditoría en las diversas etapas del proceso de expedición, permitiendo realizar un enlace biométrico entre los miembros del personal y las actividades bajo su responsabilidad.

Existen también varias aplicaciones típicas de la biometría en las fronteras.

Cada vez que un/a viajero/a (es decir, una persona titular de eMRTD) ingresa a un Estado o sale de un Estado, su identidad puede verificarse con respecto a la imagen creada cuando se expidió su documento de viaje. Esto asegurará que el portador de un documento es la persona legítima a la cual se ha expedido dicho documento y mejorará la eficacia de todo sistema de información anticipada sobre los pasajeros (API). El Estado expedidor u organización expedidora puede encontrar conveniente almacenar la plantilla o plantillas biométricas en el documento de viaje junto con la imagen, de modo que la identidad del viajero pueda verificarse en lugares del interior donde el sistema biométrico esté bajo el control del expedidor.

Verificación en ambos sentidos — Los datos actuales de la imagen biométrica captada de la persona que viaja y los datos biométricos de su documento de viaje (o de una base de datos central) pueden cotejarse (si corresponde construyendo plantillas biométricas de cada uno) para confirmar que el documento de viaje no ha sido alterado.

Verificación en tres sentidos — Los datos actuales de la imagen biométrica captada de la persona que viaja, los datos biométricos de su documento de viaje y los datos biométricos almacenados en la base de datos central pueden cotejarse (si corresponde, construyendo plantillas biométricas de cada uno) para confirmar que el documento de viaje no ha sido alterado. Esta técnica compara a la persona con su eMRTD y con la base de datos que registra los datos ingresados en el eMRTD en el momento de su expedición.

Verificación en cuatro sentidos — Una cuarta verificación confirmatoria, aunque no de carácter electrónico, consiste en cotejar visualmente los resultados de la verificación en tres sentidos con la fotografía digitalizada en la página de datos del eMRTD del viajero.

Además de las aplicaciones de inscripción y seguridad fronteriza de la biometría, manifestadas en los cotejos de uno a uno y de uno a varios, los Estados y organizaciones también deberían considerar y establecer sus propios criterios con respecto a:

- La exactitud de las funciones de cotejo biométrico del sistema. Los Estados expedidores u organizaciones expedidoras deben codificar una o más características biométricas del rostro, huellas digitales o iris en el eMRTD con arreglo a las especificaciones de la LDS. (También pueden almacenarse en una base de datos accesible al Estado receptor u organización receptora). Una vez recibida una imagen biométrica normalizada por la OACI, los Estados receptores u organizaciones receptoras deben escoger su propio soporte lógico de verificación biométrica y determinar sus propios umbrales de resultados biométricos para las proporciones de aceptación de la verificación de identidad y la identificación de impostores.

- El rendimiento (p. ej., viajeros por minuto) del sistema biométrico o del sistema de cruce de frontera en su totalidad.

- Adecuación de una determinada tecnología biométrica (rostro o dedo u ojo) a la aplicación de cruce de frontera.

3.5 Limitaciones de las soluciones biométricas

Se reconoce que la implantación de la mayoría de las tecnologías biométricas es susceptible de desarrollo ulterior. Considerando la rapidez de los cambios tecnológicos, toda especificación (incluyendo las de este volumen) debe tener en cuenta y reconocer que habrá cambios resultantes de las mejoras tecnológicas.

La información biométrica almacenada en los documentos de viaje se ajustará a todas las leyes nacionales de protección de datos o a las leyes de confidencialidad del Estado expedidor u organización expedidora.

4. SELECCIÓN DE CARACTERÍSTICAS BIOMÉTRICAS APLICABLES A LOS eMRTD

Se ha reconocido desde hace tiempo que los nombres y la reputación no son suficientes para garantizar que la persona titular de un documento de identidad (eMRTD) asignado a una persona por el Estado expedidor u organización expedidora sea la misma persona que, ante un Estado receptor u organización receptora, pretende ser el/la mismo/a titular.

El único método para relacionar irrevocablemente a la persona con su documento de viaje es contar con una característica fisiológica, es decir, una característica biométrica de dicha persona relacionada con su documento de viaje en una forma a prueba de manipulaciones indebidas.

4.1 Característica biométrica primaria: imagen facial

Codificación de las imágenes faciales de referencia

El retrato facial impreso de un MRTD conforme a las normas de la OACI es un elemento esencial de ese documento y uno de los portadores de información más importantes, que vincula el documento a su titular. Un retrato facial normalizado de alta calidad ayuda a los organismos expedidores a controlar la identidad y a los organismos fronterizos a inspeccionar el documento de viaje manualmente o mediante un proceso automatizado. Los requisitos para captar y codificar las imágenes faciales se especifican en la norma ISO/IEC 39794-5, Anexo D.1.

4.2 Otras características biométricas opcionales

Los Estados expedidores u organizaciones expedidoras pueden, con carácter opcional, ingresar datos adicionales en sus procesos de verificación de identidad (o en procesos de otros Estados) incluyendo caracteres biométricos múltiples en sus documentos de viaje, es decir, una combinación de rostro o huella digital o iris. Esto es especialmente pertinente para aquellos Estados u organizaciones que ya pueden tener bases de datos de huellas digitales o iris contra las cuales pueden verificar las características biométricas que se le presentan, por ejemplo, como parte del sistema para la expedición de tarjetas de identidad.

Almacenamiento de la biometría de la huella digital opcional

Existen tres clases de tecnología biométrica para huellas digitales: sistemas basados en la imagen de la huella, sistemas basados en detalles minuciosos de la huella y sistemas basados en la configuración de la huella. Si bien se han elaborado normas para estas clases a efectos de que la mayoría de los sistemas resulten interfuncionales dentro de la propia clase, éstos no son interfuncionales entre clases. Por consiguiente, están surgiendo tres normas de interfuncionamiento de las huellas digitales: almacenamiento de los datos de imagen, almacenamiento de los datos de detalles minuciosos y almacenamiento de datos de la configuración. Cuando un Estado expedidor u organización expedidora opta por proporcionar datos de huellas digitales en su eMRTD, el almacenamiento de la imagen de la huella digital es obligatorio para permitir el interfuncionamiento mundial entre las clases. El almacenamiento de una plantilla conexa queda a discreción del Estado expedidor u organización expedidora.

Cuando un Estado expedidor u organización expedidora opta por almacenar imágenes de huellas digitales en el CI sin contacto, el tamaño óptimo de imagen DEBERÍA ser adecuado para la verificación 1:1.

Los requisitos para captar y codificar las imágenes del dedo se especifican en la norma ISO/IEC 39794-4.

Almacenamiento de la biometría del iris opcional

Cuando un Estado expedidor u organización expedidora opta por proporcionar datos del iris en su eMRTD, el almacenamiento de la imagen del iris es obligatorio para permitir el interfuncionamiento mundial. El almacenamiento de una plantilla conexa queda a discreción del Estado expedidor u organización expedidora.

Cuando un Estado expedidor u organización expedidora opta por almacenar imágenes del iris en el CI sin contacto, el tamaño óptimo de imagen DEBERÍA ser adecuado para la verificación 1:1.

Los requisitos para captar y codificar las imágenes del iris se especifican en la norma ISO/IEC 39794-6.

5. ALMACENAMIENTO DE LOS DATOS BIOMÉTRICOS Y DE OTRO TIPO EN FORMATO LÓGICO EN UN CI SIN CONTACTO

Se EXIGE el uso de imágenes digitales y que éstas estén almacenadas electrónicamente en el documento de viaje.

5.1 Características del CI sin contacto

Un CI sin contacto de alta capacidad SERÁ el medio de almacenamiento electrónico especificado por la OACI como tecnología de ampliación de capacidad para utilizar un eMRTD con el empleo de la biometría.

Los CI sin contacto y la codificación

Los CI sin contacto utilizados en los eMRTD SE AJUSTARÁN a ISO/IEC 14443 Tipo A o Tipo B y a [ISO/IEC 7816-4]. La LDS SE CODIFICARÁ con arreglo al método de acceso aleatorio. La distancia de lectura (por combinación del eMRTD y el dispositivo lector) por lo general es de hasta 10 cm según se indica en la ISO/IEC 14443. En el Doc 9303-10 se proporciona un perfil de aplicación ISO/IEC 14443 para los MRTD.

Capacidad de almacenamiento de datos del CI sin contacto

La capacidad de almacenamiento de datos del CI queda a discreción del Estado expedidor u organización expedidora, pero SERÁ lo suficientemente grande para almacenar la imagen facial almacenada obligatoria, los datos de la ZLM duplicados y los elementos necesarios para asegurar los datos. El almacenamiento de imágenes faciales adicionales, huellas digitales o iris, puede exigir un aumento considerable de la capacidad de almacenamiento de datos. No se especifica un valor máximo de la capacidad de datos del CI sin contacto.

Almacenamiento de otros datos

Los Estados expedidores u organizaciones expedidoras PUEDEN utilizar la capacidad de almacenamiento del CI sin contacto en un eMRTD para ampliar la capacidad de los datos de lectura mecánica del eMRTD más allá del valor definido para intercambio mundial. Esto puede tener la finalidad de proporcionar acceso de lectura mecánica a la información de los documentos generadores (p. ej., detalles del certificado de nacimiento), confirmación (biométrica) de la identidad personal almacenada o detalles de verificación de la autenticidad del documento.

5.2 Estructura lógica de datos

Para asegurar el interfuncionamiento mundial de la lectura mecánica de los detalles almacenados DEBE adherirse a una estructura lógica de datos (LDS) que define el formato del registro de detalles en el CI sin contacto.

Estructura de los datos almacenados

La estructura lógica de datos se especifica en el Doc 9303-10. En dicho documento se describe en detalle la información obligatoria y opcional que ha de incluirse dentro de determinados bloques de datos biométricos en la LDS.

Datos mínimos que han de almacenarse en la LDS

Los datos mínimos obligatorios que han de almacenarse en la LDS del CI sin contacto SERÁN una duplicación de los datos de la zona de lectura mecánica en el grupo de datos 1 y de la imagen facial de la persona titular en el grupo de datos 2. Además, el CI en un eMRTD normalizado CONTENDRÁ el objeto de seguridad (EF.SOD) necesario para validar la integridad de los datos creados por el expedidor — estos se almacenan en el fichero reservado núm. 1 según se especifica en la LDS (véase el Doc 9303-10). El objeto de seguridad (EF.SOD) es la condensación de los grupos de datos en uso.

5.3 Seguridad y carácter privado de los datos almacenados

Tanto el Estado expedidor como el receptor y la organización expedidora como receptora deben cerciorarse de que los datos almacenados en el CI sin contacto no han sido alterados desde que fueron registrados en el momento de expedición del documento. Además, las leyes o prácticas de protección de la vida privada en el Estado expedidor u organización expedidora pueden exigir que solamente una persona u organización autorizada tengan acceso a dichos datos. En consecuencia, la OACI ha elaborado especificaciones, que se presentan en el Doc 9303-11 y en el Doc 9303-12 con respecto a la aplicación y uso de técnicas criptográficas modernas, en particular los programas de infraestructura de clave pública (PKI) que DEBEN emplear los Estados expedidores u organizaciones expedidoras en sus documentos de viaje de lectura mecánica con arreglo a las especificaciones establecidas en el Doc 9303. Esto está dirigido principalmente a aumentar la seguridad mediante medios automáticos de autenticación de los eMRTD y de sus titulares legítimos/as con carácter internacional. Además, se recomiendan métodos para implantar la autenticación internacional del eMRTD y posibilitar el uso de dichos documentos para facilitar aplicaciones biométricas o de comercio-e. Las especificaciones del Doc 9303-11 permiten al Estado expedidor u organización expedidora proteger los datos almacenados con respecto al acceso no autorizado mediante el método de control de acceso.

Esta edición del Doc 9303 parte del supuesto de que los datos de la LDS1 no se escribirán en los CI sin contacto después de su personalización. Por consiguiente, el proceso de personalización DEBERÁ bloquear el CI sin contacto como paso final. Una vez bloqueado el CI sin contacto (después de la personalización y antes de la expedición) solo pueden escribirse otros datos en el CI sin contacto después de la ejecución con éxito de un mecanismo de autenticación (TA), según se especifica en el Doc 9303-10 y el Doc 9303-11. Después de la expedición, un CI sin contacto bloqueado no puede desbloquearse.

Infraestructura de clave pública (*PKI)*

La finalidad del programa PKI, según se describe, consiste principalmente en permitir a las autoridades de inspección del eMRTD (Estados receptores u organizaciones receptoras) verificar la autenticidad e integridad de los datos almacenados en el eMRTD. Las especificaciones no intentan prescribir una implantación completa de una estructura PKI complicada, sino proporcionar una forma de implantación en la cual los Estados u organizaciones puedan tener opciones en varios sectores (como la autenticación activa, antidespumado de datos y control de acceso, cruce automático de fronteras, etc.), además con la posibilidad de graduar la implantación de características adicionales sin dejar de cumplir con el marco total.

Se utilizan certificados para fines de seguridad, conjuntamente con una metodología para la distribución de claves públicas (certificados) a los Estados u organizaciones y la PKI se ajusta para fines de la OACI.

Las especificaciones para la PKI se describen en detalle en el Doc 9303-12.

6. MÉTODOS DE ENSAYO PARA LOS EMRTD

La OACI, en cooperación con la ISO, ha elaborado métodos de ensayo para calificar los eMRTD con respecto a su cumplimiento de las especificaciones establecidas en el Doc 9303, Partes 9, 10, 11 y 12. Estos métodos de ensayo se especifican en los informes técnicos de la OACI y se mantienen bajo la coordinación de ISO/IEC JTC1 1/SC 17/WG 3.

SE RECOMIENDA a los Estados expedidores y organizaciones expedidoras que califiquen sus eMRTD, sistemas de inspección y soluciones PKI con arreglo a las especificaciones sobre ensayos que se indican a continuación:

ISO/IEC 18745-2	Ensayos específicos para la interfaz sin contacto de los eMRTD
OACI Informe técnico RF & PROTOCOL P3	Ensayo de la LDS y de los protocolos
OACI Informe técnico RF & PROTOCOL P4	Ensayos para los sistemas de inspección
OACI Informe técnico RF & PROTOCOL P5	Ensayos para los objetos PKI

7. REFERENCIAS (NORMATIVAS)

OACI Informe técnico RF & PROTOCOL P3	Protocolo RF y norma de ensayo de aplicación para eMRTD — Parte 3: Ensayos para el protocolo de aplicación y estructura lógica de datos
OACI Informe técnico RF & PROTOCOL P4	Protocolo RF y norma de ensayo de aplicación para eMRTD — Parte 4: Ensayo de conformidad para sistemas de inspección
OACI Informe técnico RF & PROTOCOL P5	Protocolo RF y norma de ensayo de aplicación para eMRTD — Parte 5: Ensayos para objetos PKI
ISO/IEC 2382-37	Tecnología de la información – Vocabulario – Parte 37: Biometría
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 10373-6	ISO/IEC 10373-6:2011, 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 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 radiofrecuencias. *Nota.— Las más recientes revisiones de ISO/IEC 14443-2 estipulan límites de la EMD con carácter obligatorio. No obstante, los eMRTD ya expedidos o en proceso no se ajustan necesariamente a este nuevo parámetro. Para mantener la retrocompatibilidad de cumplimiento, los límites EMD a que se hace referencia en ISO/IEC 14443-2 deberían seguir siendo OPCIONALES para los eMRTD en el marco del Doc 9303.*
ISO/IEC 14443-3	ISO/IEC 14443-3:2016 (versión corregida el 1-9-2016), 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 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 19794-6:2005, Tecnología de la información — Formatos de intercambio de datos biométricos — Parte 5: Datos de imágenes del iris
ISO/IEC 39794-4 ISO/IEC 39794-4	ISO/IEC 39794-4, 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	ISO/IEC 39794-5, 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	ISO/IEC 39794-6, Tecnología de la información— Formatos de intercambio de datos biométricos extensibles — Parte 6: Datos de imágenes del iris

— — — — — — — —

Apéndice A de la Parte 9

PROCESO DE LECTURA DE LOS eMRTD (INFORMATIVO)

A.1 PRECAUCIONES EN LA FABRICACIÓN DE EMRTD

Los Estados expedidores u organizaciones expedidoras deben asegurarse de que el proceso de fabricación de la libreta y el proceso de personalización no introducen daños imprevistos al CI o su antena. Por ejemplo, el calor excesivo en el laminado o la perforación de la imagen en la zona del CI o su antena pueden dañar el conjunto del CI. Análogamente, cuando el CI está en la cubierta anterior, el entramado del exterior de la cubierta, después de colocarse, puede también dañar el CI o las conexiones con su antena.

A.2 LECTURA DE LOS DATOS OCR Y LOS DATOS EN EL CI

Se recomienda encarecidamente que el Estado receptor u organización receptora lea tanto los datos OCR como los almacenados en el CI. Cuando un Estado expedidor u organización expedidora ha bloqueado el CI para protegerlo contra escuchas furtivas, se requiere la lectura de los datos OCR para tener acceso a los datos del CI. Es conveniente que solo se utilice un lector para ambas operaciones, estando éste equipado para leer ambas. Si el MRP se abre en la página de datos y se coloca en un lector de página completa, algunos MRP tendrán el CI situado detrás de la cara de la página de datos, mientras que otros lo tendrán en la parte de la libreta que no está en el lector de página completa.

A.3 CONSTRUCCIÓN DEL DISPOSITIVO LECTOR

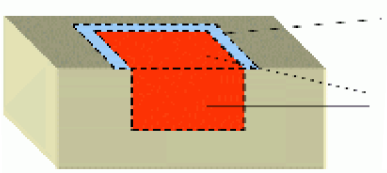
Por consiguiente, los Estados u organizaciones instalarán equipo de lectura capaz de procesar MRP de ambas geometrías, preferiblemente capaces de leer tanto los datos OCR como los del CI. En la Figura A-1 se muestran posibles configuraciones de lector capaces de leer OCR e IC. La libreta está semiabierta y dos antenas aseguran que el CI se lee independientemente de si enfrenta la ZLM o no. También se muestra una configuración menos satisfactoria en la cual el eMRTD se coloca en un lector OCR o se pasa rápidamente a través del lector OCR por deslizamiento para leer la ZLM y posteriormente en un lector de datos CI. Este arreglo será menos cómodo para el personal de inmigración.

Geometrías de lectura

Por consiguiente, los fabricantes de dispositivos lectores deben considerar la forma de diseñar las soluciones de lectura mecánica que tengan en cuenta las diversas posibilidades de orientación y que (idealmente) sean capaces de leer la ZLM y el CI sin contacto simultáneamente.

Proceso de lectura conjunta

Lector de página completa con 2 antenas orientadas perpendicularmente, o una antena grande que abarca el área de una libreta abierta



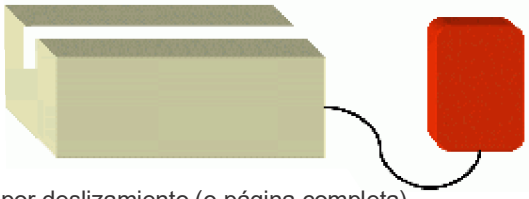
Lectura OCR

Área para lectura del CI (2 antenas o 1 antena grande)

o

Proceso de lectura en dos etapas

Lector OCR por deslizamiento o de página completa, conectado a un lector de RF separado



Lector por deslizamiento (o página completa) para lectura OCR

Lectura del CI

Primera etapa: deslizamiento del MRTD por el lector OCR o colocación sobre éste
Segunda etapa: si hay microplaqueta, colóquese el MRTD sobre el lector de CI

Figura A-1. Construcción del dispositivo lector

A.4 PROCESOS DE LECTURA

En la Figura A-2 se muestran los procedimientos de lectura de un eMRTD antes de la verificación biométrica del portador e incluyendo la misma.

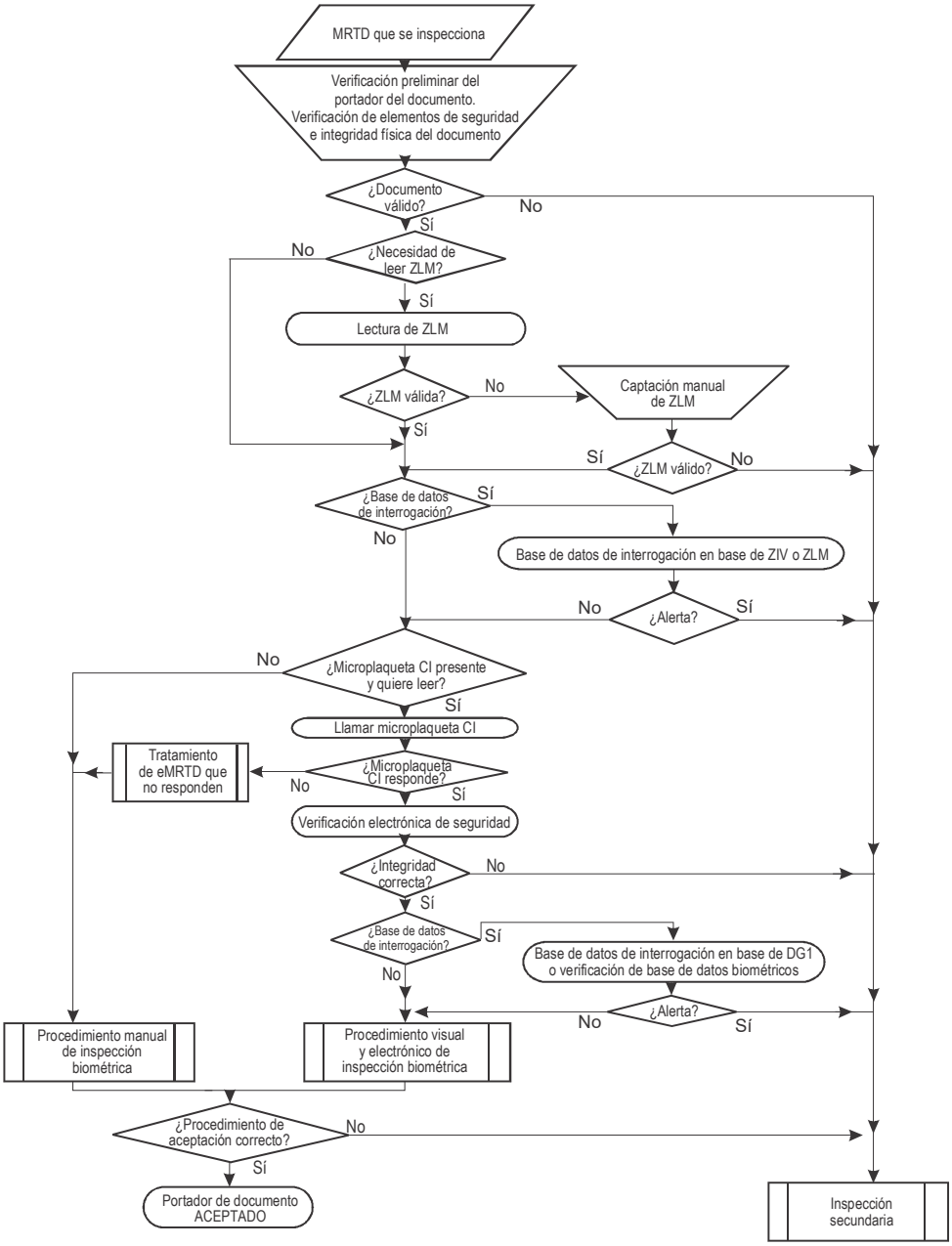


Figura A-2. Proceso de lectura del eMRTD

— FIN —

ISBN 978-92-9275-343-6