TMCASI/C.185/2016 (Rev.)

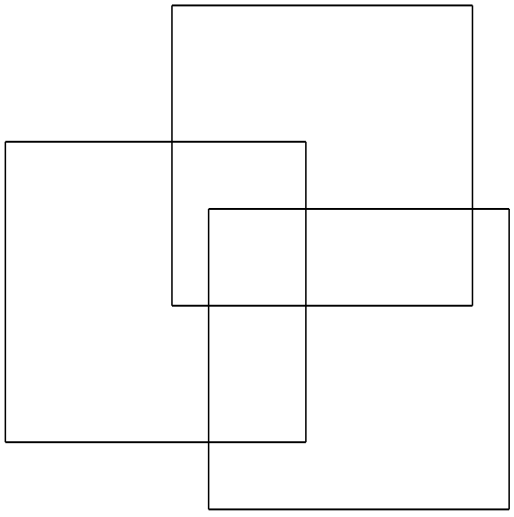
Oficina
Internacional
del Trabajo

Ginebra

Documento de referencia para la reunión del Comité Tripartito Marítimo *ad hoc* para la enmienda del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185)

(Ginebra, 10-12 de febrero de 2016)

Comentarios y propuestas de enmienda de los anexos I, II y III del Convenio núm. 185



Ginebra, 2016

Departamento
de Normas
Internacionales
del Trabajo

TMCASI/C.185/2016 (Rev.)

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO

Departamento de Normas Internacionales del Trabajo

Documento de referencia para la reunión del Comité Tripartito Marítimo *ad hoc* para la enmienda del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185)

(Ginebra, 10-12 de febrero de 2016)

Comentarios y propuestas de enmienda de los anexos I, II y III del Convenio núm. 185

Ginebra, 2016

OFICINA INTERNACIONAL DEL TRABAJO, GINEBRA

Primera edición 2016

Documento de referencia para la reunión del Comité Tripartito Marítimo ad hoc para la enmienda del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185), Ginebra, 10-12 de febrero de 2016, Oficina Internacional del Trabajo, Departamento de Normas Internacionales del Trabajo, Ginebra, OIT, 2015.

ISBN: 978-92-2-330270-2 (impreso)
ISBN: 978-92-2-330271-9 (web pdf)

Publicado también en francés: *Document de travail pour la réunion de la Commission tripartite maritime ad hoc chargée de l'amendement de la convention (no 185) sur les pièces d'identité des gens de mer (révisée), 2003,* Genève, 10-12 février 2016, ISBN 978-92-2-230270-3 (impreso), 978-92-2-230271-0 (web pdf), Ginebra, 2015; y en inglés: *Background paper for the meeting of the Ad Hoc Tripartite Maritime Committee established for the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185),* Geneva, 10–12 February 2016, ISBN 978 92-2-130270-4 (impreso), 978-92-2-130271-1 (web pdf), Ginebra, 2015.

Impreso por la Oficina Internacional del Trabajo, Ginebra, Suiza

Índice

Anexo

Lista de abreviaturas

CSCA	autoridad de certificación responsable de los certificados de firma electrónica
DCP	directorio de claves públicas
DIM	documento de identidad de la gente de mar
DV1	documento de viaje de lectura mecánica de tamaño 1
DV3	documento de viaje de lectura mecánica de tamaño 3
ICP	infraestructura de clave pública
ISO	Organización Internacional de Normalización
LDS	estructura lógica de datos
OACI	Organización de Aviación Civil Internacional
OCT	oficina central de tramitación
OIT	Organización Internacional del Trabajo
ZIV	zona de inspección visual
ZLM	zona de lectura mecánica

Introducción

1. En febrero de 2015 se celebró una Reunión tripartita de expertos sobre el Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185), con objeto de analizar las dificultades surgidas con respecto a la aplicación de dicho Convenio — especialmente en relación con los datos biométricos (basados en la tecnología relativa a las huellas dactilares) que el Convenio exige que se incluyan en el documento de identidad de la gente de mar (DIM) [1]. Una clara mayoría de los expertos asistentes a esta reunión de tres días de duración concluyó que el medio más viable para avanzar era que la Conferencia Internacional del Trabajo enmendara el anexo I del Convenio y, de ser necesario, los demás anexos de ese instrumento, con objeto de que se armonizaran las disposiciones relativas a los datos biométricos del Convenio núm. 185 con las normas de la Organización de Aviación Civil Internacional (OACI), que son de aplicación universal para los documentos de viaje y otros documentos similares.

2. Por consiguiente, la Reunión de expertos solicitó al Consejo de Administración de la Oficina Internacional del Trabajo que convocara en 2016 una reunión del «órgano marítimo tripartito debidamente constituido», de conformidad con lo dispuesto en el párrafo 1 del artículo 8 del Convenio, a fin de asesorar a la Conferencia Internacional del Trabajo sobre la adopción de enmiendas a los anexos del Convenio y formuló la siguiente recomendación [2]:

> Recomendación 1: La Oficina Internacional del Trabajo debería preparar un proyecto preliminar de revisión de los anexos I y II del Convenio núm. 185, por el que se modifica el modelo biométrico correspondiente a la plantilla de huellas dactilares integradas en un código de barras bidimensional, sustituyéndolo por una imagen facial almacenada en un chip electrónico sin contacto, y requiriéndose que la base electrónica de datos nacional contenga únicamente las claves públicas exigidas para verificar las firmas digitales integradas en un chip sin contacto definidas en el documento núm. 9303 de la OACI. Se prevé la supresión de todas las referencias a normas técnicas distintas de las que figuran en el documento núm. 9303 de la OACI, habida cuenta de que todas las normas ISO pertinentes ya se remiten al documento núm. 9303 de la OACI. Las referencias al documento núm. 9303 deberían mencionar dicho documento, incluidas las enmiendas que puedan adoptarse posteriormente, de manera que en el futuro no sea necesario modificar los anexos, a medida de que la OACI elabore nuevas versiones del documento núm. 9303 y del avance de la tecnología relativa al pasaporte electrónico. En el caso de que las enmiendas a los anexos I y II requieran introducir modificaciones a los procesos y procedimientos previstos en el anexo III (por ejemplo, la necesidad de asegurar la calidad de la fotografía del marino), podría ser necesario incluirlas en un proyecto preliminar de revisión del anexo III.

3. En su 323.ª reunión (marzo de 2015), el Consejo de Administración tomó nota de la conclusión general y de las recomendaciones de la Reunión tripartita de expertos y decidió convocar una reunión del Comité Marítimo Tripartito *ad hoc* para que formulara propuestas, basadas en las recomendaciones de la Reunión de expertos, a fin de someterlas

[1] La información sobre la Reunión, incluidos los documentos de referencia y el informe sobre las discusiones mantenidas, está disponible en la página web del Convenio sobre el trabajo marítimo, 2006, de la OIT: http://www.ilo.org/global/standards/maritime-labour-convention/events/WCMS_301229/lang--es/index.htm.

[2] OIT: *Resultados de la Reunión de expertos relativa al Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185) (Ginebra, 4-6 de febrero de 2015)*, Consejo de Administración, 323.ª reunión, Ginebra, marzo de 2015, documento GB.323/LILS/4. La conclusión general y las recomendaciones de la Reunión de expertos figuran en el anexo de dicho documento.

a la consideración de la Conferencia Internacional del Trabajo en su 105.ª reunión (2016), en un punto del orden del día titulado «Enmienda de los anexos del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185)» [3].

4. Para ayudar al Comité Marítimo Tripartito *ad hoc* y tal como recomendó la Reunión de expertos en febrero de 2015, la Oficina ha preparado un proyecto preliminar de propuestas (en adelante, «proyecto preliminar») para la enmienda de los anexos I y II del Convenio núm. 185 (y para el correspondiente ajuste del anexo III) donde se indican claramente todos los cambios con respecto a la versión vigente de los anexos. El proyecto preliminar figura en la parte I del presente documento de referencia. En la parte II se explican los principales cambios que los gobiernos deberían introducir en la aplicación del Convenio núm. 185, sobre todo en relación con el sistema de expedición de DIM, si la Conferencia Internacional del Trabajo adoptara en junio de 2016 las enmiendas propuestas en el proyecto preliminar.

5. Por consiguiente, se invita al Comité Marítimo Tripartito *ad hoc* a proponer a la Conferencia Internacional del Trabajo enmiendas a los anexos del Convenio núm. 185, sobre la base del proyecto preliminar que figura en la parte I *infra* y tomando en consideración las explicaciones incluidas en la parte II.

6. Otra recomendación de la Reunión tripartita de expertos, de la que el Consejo de Administración tomó nota, estaba relacionada con la fecha de entrada en vigor de las enmiendas de los anexos y las disposiciones transitorias. Esta recomendación, que se basaba principalmente en el párrafo 1 del artículo 3 del Convenio [4], establecía lo siguiente:

> Recomendación 6: Debido a la importancia de reforzar el sistema de DIM en vigor y de aplicar al mismo tiempo los cambios registrados en el ámbito de la tecnología, debería establecerse un período de transición adecuado.
>
> *Entrada en vigor y período de transición*
>
> *Entrada en vigor*
>
> 1. Las enmiendas entrarán en vigor transcurrido un año desde su adopción por la Conferencia Internacional del Trabajo de conformidad con el párrafo 1 del artículo 8 del Convenio.
>
> *Período de transición*
>
> 2. Los Miembros cuya ratificación del Convenio se haya registrado con anterioridad a la fecha de la entrada en vigor a la que se hace referencia en el párrafo 1, *supra*, podrán, durante un período no mayor de tres años después de su entrada en vigor, seguir expidiendo los DIM de conformidad con el texto del Convenio anterior a la enmienda de sus anexos.
>
> *Disposición de protección*
>
> 3. La entrada en vigor de las enmiendas o el vencimiento de los períodos anteriores de transición no afectarán la validez de los DIM expedidos durante el período de vigencia de las disposiciones anteriores. Estas disposiciones seguirán en vigor hasta su fecha de vencimiento o hasta la fecha de renovación del DIM, de conformidad con el artículo 3, párrafo 6, del Convenio, si esa fecha es posterior.

[3] OIT: *Actas de la 323.ª reunión del Consejo de Administración de la Oficina Internacional del Trabajo*, Consejo de Administración, 323.ª reunión, Ginebra, marzo de 2015, documento GB.323/PV, párrafo 360.

[4] Véanse también el párrafo 2 del artículo 4 y el párrafo 3 del artículo 5 del Convenio.

7. El Comité Marítimo Tripartito *ad hoc* tal vez estime oportuno confirmar que está de acuerdo con la recomendación 6 relativa al calendario propuesto para la entrada en vigor de las enmiendas propuestas y las disposiciones transitorias propuestas.

8. En la parte III del presente documento de referencia se presentan varias opciones sobre cómo pueden aplicar los Miembros ratificantes un sistema de expedición de DIM económicamente viable con arreglo a los anexos enmendados. Si bien no se requiere que el Comité Marítimo Tripartito *ad hoc* tome una decisión a ese respecto, puesto que la decisión sobre tales cuestiones compete a cada Miembro, antes de proponer enmiendas a la Conferencia Internacional del Trabajo, el Comité debería tener la certeza de que tales enmiendas permitirían, en la práctica, que los Miembros ratificantes aplicaran plenamente el Convenio núm. 185.

I. Proyecto preliminar de enmienda de los anexos

9. El anexo I del Convenio, titulado «Modelo para el documento de identidad de la gente de mar», se reemplazaría por completo por el texto siguiente. Las notas a pie de página del editor figuran únicamente a título informativo y no formarían parte del texto final del anexo.

Anexo I

Modelo para el documento de identidad de la gente de mar

A reserva de los requisitos primordiales que se establecen en el artículo 3 de este Convenio, el documento de identidad de la gente de mar (DIM), cuya forma y contenido se describen a continuación, se ajustará — en lo que respecta a los materiales utilizados para su elaboración y la presentación y el almacenamiento de los datos que contiene — a los requisitos obligatorios para los documentos oficiales de viaje de lectura mecánica de tamaño 1 (DV-1), previstos en el documento núm. 9303 de la Organización de Aviación Civil Internacional (OACI) sobre documentos de viaje de lectura mecánica, teniendo plenamente en cuenta cualesquiera recomendaciones u orientaciones enunciados en dicho documento. El término «documento núm. 9303» se entenderá como referencia a la séptima edición (2015) del documento publicado por la OACI, con las posibles modificaciones que pudieran introducirse de conformidad con los procedimientos conexos de la OACI. Las referencias en el presente anexo a disposiciones particulares del documento núm. 9303 se refieren a la séptima edición del mismo, pero se entenderá que también hacen referencia a las disposiciones correspondientes de cualesquiera ediciones posteriores. El Director General de la Oficina Internacional del Trabajo podrá ocasionalmente, a petición del Consejo de Administración, elaborar pautas de orientación para los Miembros en relación con las disposiciones específicas del documento núm. 9303 que deben tomarse en consideración.

El DIM será un documento de identidad de lectura mecánica de tamaño 1 (DV-1) con las características físicas que se indican en la sección 2 de la parte 3 del documento núm. 9303, «Especificaciones comunes a todos los documentos de viaje de lectura mecánica». La impresión y la tipografía empleadas tanto en la zona de inspección visual como en la zona de lectura mecánica se ajustarán a lo dispuesto en las secciones 3 y 4, respectivamente, de la parte 3 del documento núm. 9303. El tamaño del documento de identidad se ajustará a las características especificadas en la sección 2 de la parte 5 del documento núm. 9303, «Especificaciones para documentos oficiales de viaje de lectura mecánica de tamaño 1 (DV-1)» y la disposición de todos los datos será conforme a las especificaciones previstas en la sección 3 de la parte 5.

El DIM incluirá un circuito integrado sin contacto, con una capacidad de almacenamiento de datos de al menos 32 kilobytes, codificados y firmados digitalmente de conformidad con las partes 9, 10, 11 y 12 del documento núm. 9303. El circuito integrado sin contacto cumplirá todos los requisitos relativos a la estructura lógica de datos (LDS) establecidos en la parte 10 del documento núm. 9303, aunque únicamente incluirá los datos obligatorios. La confidencialidad de los datos almacenados en el circuito integrado sin contacto estará protegida por un mecanismo de control de acceso, tal como se describe en la parte 11 del documento núm. 9303. La información almacenada en la LDS se limitará a los metadatos y archivos necesarios para el funcionamiento del circuito integrado y sus elementos de seguridad, así como los siguientes datos, que pueden leerse a simple vista, en las zonas de inspección visual y de lectura mecánica del DIM:

i) en el grupo de datos 1 de la LDS: una duplicación de los datos que figuran en la zona de lectura mecánica, y que se enumeran más abajo;

ii) en el grupo de datos 2 de la LDS: la representación biométrica exigida en el párrafo 8 del artículo 3 del presente Convenio, que se ajustará a lo dispuesto en la parte 9 del documento núm. 9303, bajo el epígrafe «Identificador biométrico principal: imagen facial». La imagen facial del marino será una copia de la fotografía a la que se hace referencia en el apartado *o) infra*, pero comprimida a un tamaño de entre 15 y 20 kilobytes;

iii) el objeto de seguridad del documento, que es necesario para validar la integridad de los datos almacenados en la LDS utilizando la infraestructura de clave pública de la OACI, tal como se define en la parte 12 del documento núm. 9303.

El DIM estará protegido frente a toda alteración, sustitución de la fotografía u otra actividad fraudulenta mediante el cumplimiento de los requisitos establecidos en la parte 2 del documento núm. 9303, bajo el epígrafe «Especificaciones para la seguridad del diseño, la manufactura y la expedición de documentos de viaje de lectura mecánica (DVLM)». Éste estará protegido por al menos tres elementos de seguridad física de los que se enumeran en la lista que figura en el anexo A de la parte 2 del documento núm. 9303. Algunos ejemplos de estos elementos de seguridad son:

- elementos ópticamente variables [5] en el sustrato o laminado del documento de identidad;
- elementos táctiles [6] en el sustrato del documento de identidad;
- perforaciones con láser [7] en el sustrato;
- diseño de Guilloche a dos tintas [8] en el fondo del documento de identidad;
- texto en microimpresión [9] en el fondo;
- tinta fluorescente ultravioleta;
- tinta con propiedades ópticamente variables;
- imagen esteganográfica [10] incorporada al documento de identidad.

Los datos que debe incluir el documento de identidad y su disposición en las diferentes zonas descritas en la parte 5 del documento núm. 9303 se exponen a continuación; en el DIM no deberá constar ninguna otra información:

a) Estado expedidor: nombre completo, en la zona I, sin la leyenda del campo;

b) tipo de documento: «DIM», en la zona I, sin la leyenda del campo;

c) símbolo de microplaqueta contenida, tal como se describe en la sección 2.3 de la parte 9 del documento núm. 9303: en la zona I, sin la leyenda del campo;

d) nombre completo del titular, en un solo campo, compuesto por el identificador primario seguido de una coma, a continuación un espacio y después el identificador secundario, tal como se define en la parte 5 del documento núm. 9303: en la zona II, con la leyenda del campo;

e) sexo del titular consignado con una única letra, «F» para el femenino, «M» para el masculino o «X» si no se especifica: en la zona II, con la leyenda del campo;

[5] Nota del editor: Un elemento ópticamente variable es una imagen o elemento cuya apariencia en cuanto al color o al diseño cambia según el ángulo de iluminación o de observación.

[6] Nota del editor: Un elemento táctil es un elemento superficial del documento que al tocarlo produce una «sensación» singular.

[7] Nota del editor: Una perforación con láser es un proceso mediante el cual se crean números, letras o imágenes al perforar el sustrato con láser.

[8] Nota del editor: Un diseño de Guilloche es un patrón de líneas finas continuas, generalmente creadas por computadora, que forman una imagen de naturaleza única que sólo puede volverse a originar con exactitud si se tiene acceso al equipo, al soporte lógico y a los parámetros empleados para crear el diseño original.

[9] Nota del editor: La microimpresión es un texto o símbolos impresos de un tamaño inferior a 0,25 mm/0,7 puntos de pica.

[10] Nota del editor: La esteganografía es la utilización de una imagen o información codificada u oculta dentro de una imagen visual primaria.

f) nacionalidad del titular, mediante el código de tres letras del país establecido por la Organización Internacional de Normalizacion (ISO): en la zona II, con la leyenda del campo;

g) fecha de nacimiento del titular, en formato DDbMMbAAAA, en el que «b» es un espacio en blanco (por ejemplo, 23 03 1982): en la zona II, con la leyenda del campo;

h) lugar de nacimiento del titular: en la zona II, con la leyenda del campo;

i) cualquier característica física especial que ayude a la identificación del titular: en la zona II, con la leyenda del campo. Si la autoridad expedidora decide no indicar ninguna característica identificativa o si el titular no tiene ninguna característica identificativa particular, este campo puede completarse con el término inglés «None»;

j) número único de documento asignado al DIM por la autoridad expedidora, de no más de nueve caracteres: en la zona III, con la leyenda del campo;

k) fecha de expedición del DIM, en formato DDbMMbAAAA, en el que «b» es un espacio en blanco (por ejemplo, 31 05 2014): en la zona III, con la leyenda del campo;

l) fecha de caducidad del DIM, en formato DDbMMbAAAA, en el que «b» es un espacio en blanco (por ejemplo, 31 05 2019): en la zona III, con la leyenda del campo;

m) lugar de expedición del DIM: en la zona III, con la leyenda del campo;

n) firma o marca habitual del titular: en la zona IV, sin la leyenda del campo;

o) fotografía del titular, conforme a las especificaciones para fotografías establecidas en la parte 3 del documento núm. 9303: en la zona V, sin la leyenda del campo;

p) la siguiente mención en inglés, en la zona VI, en el reverso del documento de identidad, sin la leyenda del campo:

«This document is a seafarers' identity document for the purpose of the Seafarers' Identity Documents Convention (Revised), 2003, of the International Labour Organization. This document is a stand-alone document and not a passport.»;

q) nombre de la autoridad expedidora, e información de contacto (número de teléfono, incluido el código del país, o URL de la página web, o ambas cosas) del centro permanente de coordinación designado en virtud del párrafo 4 del artículo 4 del presente Convenio: en la zona VI, en el reverso del documento de identidad, con la siguiente leyenda en inglés: «Issuing authority contact details»;

r) zona de lectura mecánica de tres líneas impresa en la zona VII, como se especifica en la sección 4 de la parte 3 y la sección 4.2 de la parte 5 del documento núm. 9303, que incluirá todos los datos obligatorios especificados en la sección 4.2 de la parte 5; los dos primeros caracteres de la línea superior de lectura mecánica serán «IS» («I» indica que se trata de un documento de identidad y «S» — que corresponde a *seafarer*, «marino» en inglés — indica que es un documento de identidad de la gente de mar).

10. El texto que figura a continuación indica las modificaciones propuestas para el anexo II del Convenio.

Anexo II

Base electrónica de datos

Los datos que deberán suministrarse para cada asiento abierto en la base electrónica de datos, que todos los Miembros habrán de mantener al día en virtud de los párrafos 1, 2, 6 y 7 del artículo 4 del presente Convenio, serán exclusivamente los siguientes:

Sección 1

1. ~~Autoridad expedidora indicada en el~~ Estado expedidor, tal como conste en la zona de inspección visual del documento de identidad de la gente de mar (DIM).

2. Nombre completo del marino, tal como conste en la zona de inspección visual del DIM ~~el documento de identidad~~.

3. Número único del documento de nueve caracteres asignado al DIM.

4. Fecha de caducidad, suspensión o retiro del ~~documento de identidad~~ DIM, escrita en el formato DDbMMbAAAA, en el que «b» es un espacio en blanco (por ejemplo, 31 05 2019).

Sección 2

5. ~~Plantilla biométrica que figure en el documento de identidad.~~ Imagen facial comprimida del marino, tal como conste en el circuito integrado sin contacto del DIM.

6. Fotografía del marino, tal como aparezca en la zona de inspección visual del DIM.

7. Pormenores sobre toda solicitud de información acerca de los ~~documentos de identidad de la gente de mar~~ DIM.

11. Se propone añadir el párrafo subrayado que figura más abajo en el anexo III del Convenio.

Anexo III

Requisitos, procedimientos y prácticas recomendados en relación con la expedición de los documentos de identidad de la gente de mar

En el presente anexo se enuncian los requisitos mínimos relativos a los procedimientos que, de conformidad con el artículo 5 del presente Convenio, deberán adoptar todos los Miembros para la expedición de los documentos de identidad de la gente de mar (en adelante «DIM»), incluidos los procedimientos de control de calidad.

En la Parte A se enuncian los resultados obligatorios que, como mínimo, debe conseguir cada Miembro al aplicar un sistema de expedición de DIM.

En la Parte B se recomiendan los procedimientos y prácticas que permitirán alcanzar dichos resultados. Aunque esta Parte no reviste carácter obligatorio, los Miembros deberán tenerla plenamente en cuenta.

No obstante lo anterior, a los efectos de la aplicación de la Parte A, los Miembros observarán todos los requisitos obligatorios pertinentes previstos en el documento núm. 9303 de la Organización de Aviación Civil Internacional (OACI). El término «documento núm. 9303» se entenderá como referencia a la séptima edición (2015) del documento publicado por la OACI, con las posibles modificaciones que pudieran introducirse de conformidad con los procedimientos conexos de la OACI. Además de tener plenamente en cuenta la Parte B del presente anexo, los Miembros darán plena consideración a las recomendaciones u orientaciones pertinentes que figuren en el documento núm. 9303, en particular en la parte 2 de dicho documento y en sus anexos.

Parte A. Resultados obligatorios

[No se propone ninguna modificación para la parte A del anexo III.]

Parte B. Procedimientos y prácticas recomendados

[No se propone ninguna modificación para la parte B del anexo III.]

II. Principales cambios en el DIM y en el proceso de expedición a raíz de las modificaciones propuestas

A. Formato, disposición y materiales de la tarjeta

12. El anexo I del Convenio núm. 185 permite actualmente que el DIM tenga el tamaño de una tarjeta de crédito (DV1) o de una página de pasaporte (DV3). Si bien este último formato deja margen para incluir más información en el DIM, resulta en cambio menos práctico para los marinos ya que no puede llevarse fácilmente en una billetera o en otro tipo de tarjetero.

13. En el proyecto preliminar de la parte I se propone que sólo deberían autorizarse documentos en formato DV1. La razón de ello es que el DIM tendría que fabricarse utilizando un sustrato que permita implantar un circuito integrado sin contacto y una antena, y que un documento de tamaño pasaporte, de una sola página (DV3), puede doblarse más fácilmente, lo que podría reducir la vida útil del circuito integrado. En dicho proyecto preliminar también se propone eliminar el código de barras bidimensional ya que ello dejaría más espacio disponible en el reverso de un DIM en formato DV1. Esto quiere decir que ya no es necesario disponer de un documento en un formato más grande (DV3) para incluir todos los datos requeridos y su traducción.

14. El proyecto preliminar hace referencia a las siete zonas indicadas en el documento núm. 9303, a saber:

- Zona I: Encabezamiento (obligatorio)
- Zona II: Datos personales (obligatorios y opcionales)
- Zona III: Datos del documento (obligatorios y opcionales)
- Zona IV: Firma o marca habitual del titular (obligatoria)
- Zona V: Elemento de identificación (obligatorio)
- Zona VI: Datos opcionales (reverso de la tarjeta)
- Zona VII: Zona de lectura mecánica (ZLM) obligatoria (reverso de la tarjeta)

Las zonas I-VI constituyen la zona de inspección visual (ZIV).

15. El DIM tendría que estar fabricado con un sustrato suficientemente resistente para proteger el circuito integrado sin contacto en su uso normal. El PVC o el policarbonato son dos opciones excelentes para el material de la tarjeta; en cualquier caso, ya no podrían expedirse DIM en papel laminado dado que este soporte no es suficientemente rígido y la antena del circuito integrado podría romperse con facilidad. Con arreglo a las propuestas que figuran en el proyecto preliminar, la disposición de los datos impresos en el DIM (nombre, fecha de nacimiento, etcétera) sería prácticamente idéntica a la prevista en la versión actual del anexo I del Convenio. Aunque los principales datos que habrán de constar también serían muy similares, en el proyecto preliminar se han propuesto algunos cambios con el objeto de garantizar que su presentación sea plenamente conforme con la

indicada en la última edición del documento núm. 9303 [11]. Así pues, convendría que todas las autoridades responsables de la expedición de los DIM se aseguraran de que la presentación de cada dato y la leyenda de campo (o la ausencia de leyendas) coinciden exactamente con la descripción que figura en la lista de la versión revisada del anexo I. En al anexo al presente documento se presenta un ejemplo de DIM que recoge todos los elementos indicados.

16. Todos los DIM deben contener un número suficiente de elementos de seguridad para garantizar la protección contra el fraude. Si bien los elementos de seguridad digitales ya forman parte del circuito integrado, el DIM también debe incluir elementos de seguridad física para aquellos casos en que la entidad que verifica la identidad de la gente de mar no tenga acceso a lectores de pasaportes electrónicos conectados a la infraestructura de clave pública (ICP) para verificar la seguridad digital. La versión actual del anexo I sólo exige un elemento de seguridad de una lista muy restringida. De conformidad con el proyecto preliminar, la versión revisada del anexo I exigiría como mínimo tres elementos de seguridad del anexo A de la parte 2 del documento núm. 9303. Muchos documentos de identidad utilizarán más de tres elementos de seguridad física, y la entidad encargada de facilitar los documentos podrá informar sobre todos los elementos de seguridad de un documento en particular; en cualquier caso, es importante garantizar que por lo menos tres de esos elementos de seguridad física correspondan a los que figuran en la lista del anexo A de la parte 2 del documento núm. 9303.

B. Elementos biométricos y registro de datos biométricos

17. Una de las diferencias más importantes en relación con el texto actual de los anexos del Convenio núm. 185 es que la «plantilla u otra representación biométrica del titular» exigida en el párrafo 8 del artículo 3 del Convenio ya no sería una huella dactilar impresa en forma de números en un código de barras sino un «Identificador biométrico principal: imagen facial» definido en la parte 9 del documento núm. 9303. Este cambio incidiría considerablemente en la aplicación del Convenio núm. 185, tanto en lo que concierne a la expedición de los DIM como a su verificación en los puertos y pasos fronterizos.

18. En primer lugar, dicho cambio respondería al desafío de lograr la interoperabilidad, es decir, garantizar que los datos biométricos incluidos en un DIM expedido en cualquier país ratificante puedan verificarse en todos los demás países. Dado que para la verificación biométrica de un marino se utilizaría el reconocimiento facial en lugar del reconocimiento de las huellas dactilares, la OIT ya no tendría que garantizar la interoperabilidad mediante la elaboración de una lista de productos biométricos que haya sometido a prueba para establecer su conformidad con los requisitos del Convenio. El «Identificador biométrico principal: imagen facial» definido en el documento núm. 9303 consiste en una representación comprimida y formateada del rostro del marino. Todos los productos de reconocimiento facial disponibles pueden trabajar con imágenes de este tipo, y la OACI, las autoridades expedidoras de pasaportes y las autoridades fronterizas de todo el mundo ya están buscando soluciones a los problemas de interoperabilidad.

19. En segundo lugar, esta modificación supondría que para la expedición del DIM ya no sería indispensable la presencia del marino para obtener sus huellas dactilares. Ello permitiría el envío del DIM a través del correo postal u otro sistema de correo seguro sin necesidad de que el marino acuda a una oficina. Es evidente que, al expedir un DIM por primera vez, el marino deberá personarse para que un funcionario verifique su condición de marino y

[11] El texto de todas las partes del documento núm. 9303, séptima edición, 2015, puede descargarse en http://www.icao.int/publications/pages/publication.aspx?docnum=9303.

compruebe que la fotografía utilizada para sus datos biométricos es la de esa misma persona. Ahora bien, para la renovación del documento, bastaría con que el marino enviara una solicitud, adjuntando el antiguo DIM y una nueva fotografía. La fotografía podría compararse con la que figura en el antiguo DIM y con la imagen del marino que se conserva en la base electrónica de datos nacional a fin de verificar que se trata de una representación fidedigna de la misma persona. Tras ello podría expedirse el nuevo DIM y enviarse por correo a su titular. Esto último sería facultativo y las autoridades pertinentes aún podrían exigir la presencia del marino tanto para la expedición inicial del documento como para su renovación ulterior.

20. Como el proceso de expedición del documento ya no requeriría la toma de huellas dactilares, los correspondientes equipos y programas informáticos resultarían innecesarios. La imagen facial puede obtenerse tomando una fotografía o bien escaneando una fotografía impresa. Más importante aún, el proceso de verificación ya no requeriría equipos y programas informáticos para la lectura de huellas dactilares, y podría llevarse a cabo utilizando la misma infraestructura que ya está disponible en los puestos fronterizos para comprobar la identidad de los titulares de pasaportes electrónicos.

21. La utilización de la imagen facial como identificador biométrico del titular del DIM obligaría a la autoridad expedidora a conceder más importancia que antes a la calidad de la imagen. Los datos trasmitidos recientemente a la Organización Internacional de Normalización (ISO) procedentes de los sistemas automáticos de control fronterizo de Australia y Nueva Zelandia muestran que el rendimiento de los algoritmos de reconocimiento facial utilizados en los sistemas de control fronterizo varía significativamente dependiendo del país que haya expedido el pasaporte electrónico. En la mayoría de los casos, esta diferencia en el rendimiento tiene que ver al parecer con la calidad de la imagen del pasaporte electrónico. La ISO todavía está elaborando nuevas recomendaciones sobre la base de estos datos; no obstante, se han identificado varias cuestiones que todas las autoridades expedidoras deberían tener muy presentes al tomar las fotografías de los marinos o al considerar si aceptan o rechazan las fotografías que éstos presentan para utilizarlas en sus respectivos DIM:

a) Es indispensable seguir las directrices relativas a la expresión facial, la iluminación y los tocados que se indican en la sección 3.9 de la parte 3 del documento núm. 9303. En caso de que la imagen facial captada en vivo o la fotografía facilitada no respeten estas directrices habrá que rechazarlas y tomar o solicitar otra fotografía.

b) Aunque el documento núm. 9303 no lo exige, se recomienda encarecidamente que al tomar las fotografías los marinos no lleven gafas graduadas o de lectura, ni siquiera en el caso de que las utilicen habitualmente.

c) Al recortar una fotografía o escanear una fotografía impresa es importante asegurarse de que en la fotografía recortada no aparezcan líneas de separación entre fondos de color diferente (por ejemplo el color de fondo del escáner y el color de fondo de la fotografía). Toda línea nítida vertical u horizontal que aparezca en el fondo tendrá un efecto negativo en la calidad de la imagen una vez haya sido comprimida para su almacenamiento en el circuito integrado sin contacto.

d) La compresión únicamente debería hacerse una vez, por lo que las imágenes escaneadas originales deberán almacenarse utilizando la máxima resolución del escáner y comprimirse ulteriormente para su almacenamiento en el circuito integrado sin contacto.

e) Los procedimientos de control de calidad siempre deberían incluir una etapa para visualizar la imagen almacenada en el circuito integrado a fin de garantizar que ésta tiene la calidad requerida y concuerda con la imagen impresa en el DIM.

C. Codificación del circuito integrado

22. Según el proyecto preliminar, el anexo I ya no exigiría la utilización de un código de barras bidimensional. En su lugar, los datos de los marinos, incluida la información biométrica, se almacenarían en un circuito integrado sin contacto. Ello significa que, de revisarse los anexos según lo previsto, todas las autoridades expedidoras de DIM tendrían que añadir una nueva etapa al proceso de expedición a fin de codificar los datos necesarios en una estructura lógica de datos (LDS) contenida en el circuito integrado sin contacto. Ello constituiría una parte del proceso de personalización por el que un documento en blanco se convierte en un DIM acabado con los datos personales del titular.

23. La nueva etapa de codificación de la tarjeta en el proceso de personalización implica que ahora es de importancia capital cerciorarse de que los datos impresos en el DIM concuerden con los datos almacenados en el circuito integrado sin contacto. Idealmente, la codificación del circuito integrado y la impresión de los DIM deberían llevarse a cabo en una sola etapa, utilizando para ello una impresora que también sea capaz de codificar el circuito integrado sin contacto. De no ser posible, habría que asegurarse de que el programa informático utilizado para la expedición hace un seguimiento adecuado de cada documento cuando éstos pasan de la etapa de impresión a la etapa separada de codificación o viceversa. En ambos casos habría que prever una nueva etapa de garantía de la calidad en el proceso de expedición, en la que se cotejarían los datos almacenados en el circuito integrado sin contacto y los datos impresos en la tarjeta (tanto en la zona de inspección visual (ZIV) como en la zona de lectura mecánica (ZLM)) con el objeto de verificar que los tres conjuntos de datos personales del marino (en la ZIV, la ZLM y en el circuito integrado) y las dos fotografías (la que aparece impresa en la ZIV y la que se almacena en el circuito integrado) son iguales.

24. La utilización del circuito integrado sin contacto también implica que sería preciso disponer de nuevas máquinas para cumplir lo dispuesto en el párrafo 9 del artículo 3 del Convenio núm. 185, donde se indica, entre otras cosas, que «los marinos deberán tener fácil acceso a las máquinas que les permitan examinar los datos que se refieran a ellos y no puedan leerse a simple vista». En la práctica, esto requeriría que la autoridad expedidora implantara un sistema que pudiera leer y mostrar en una pantalla los datos almacenados en el circuito integrado para que el marino pueda verificarlos. Podría emplearse el mismo sistema utilizado para la garantía de la calidad mencionado en el párrafo anterior, ya que éste mostraría tanto la información almacenada en el circuito integrado como la información de la ZLM y la ZIV, a fin de que el marino pueda verificar fácilmente si todos sus datos personales son correctos.

25. Conviene destacar que la introducción del circuito integrado sin contacto y de los correspondientes equipos para su codificación y lectura incrementaría el costo del sistema de expedición de los DIM y de cada DIM que se produzca. La contrapartida, sin embargo, sería que en muchos pasos fronterizos ya existe la infraestructura para leer y decodificar la información almacenada en el circuito integrado de conformidad con lo indicado en el documento núm. 9303, mientras que prácticamente no existe la infraestructura para leer y decodificar los códigos de barras bidimensionales.

26. Dado que el circuito integrado sin contacto y su antena están ocultos en la tarjeta que se somete al proceso de personalización hasta obtener un DIM acabado, las autoridades expedidoras tendrían que adquirir DIM en blanco dotados de circuitos integrados sin contacto adecuados, y no podrían utilizar las existencias de tarjetas que hubieran adquirido para su utilización según lo dispuesto en las versiones actuales de los anexos del Convenio núm. 185. Asimismo, habría que asegurarse de que los circuitos integrados sin contacto que se utilizan en los DIM son plenamente compatibles con los requisitos indicados en el documento núm. 9303, en particular en las partes 10, 11 y 12. Para ello lo más fácil sería

adquirir circuitos integrados que ya hayan sido utilizados en un sistema anterior de expedición de pasaportes electrónicos.

27. Los detalles específicos de la estructura de los grupos de datos en la LDS de un circuito integrado sin contacto se indican en la parte 10 del documento núm. 9303; se trata de una estructura de grupos de datos relativamente simple, habida cuenta de que en los anexos revisados del Convenio núm. 185 que se proponen sólo se utilizarían los grupos de datos 1 y 2, así como el objeto de seguridad del documento (EF.SOD). Ahora bien, el circuito integrado sin contacto debería cumplir todas normas de la ISO relativas a los documentos de viaje electrónicos de lectura mecánica basados en circuitos integrados sin contacto de proximidad que se enumeran en la parte 10 del documento núm. 9303, lo que significa que la codificación de los grupos de datos en un circuito integrado simple de sólo lectura no sería suficiente. El circuito integrado sin contacto tendría que ser compatible con los métodos de acceso y los protocolos de seguridad necesarios, de ahí que deba ser un circuito integrado que haya sido sometido a prueba para su utilización en pasaportes electrónicos.

28. También son muy complejos los métodos utilizados para la protección de los datos almacenados en el circuito integrado sin contacto y para garantizar que dichos datos han sido inscritos por una autoridad expedidora competente; por tal motivo, las autoridades responsables de la expedición de los DIM tendrían que utilizar circuitos integrados, así como programas informáticos para las firmas digitales y la generación de certificados criptográficos, que hayan sido sometidos a prueba para su utilización en pasaportes electrónicos. Los detalles relativos a los mecanismos de seguridad y los sistemas criptográficos se presentan en las partes 11 y 12 del documento núm. 9303; probablemente éstas sean las etapas técnicamente más complejas del proceso de expedición de un DIM con arreglo a lo dispuesto en el documento núm. 9303. La utilización de la infraestructura de clave pública (ICP) en particular, que exigiría algunos esfuerzos por parte de las autoridades expedidoras, se examina a continuación de forma más detallada.

D. Infraestructura de clave pública

29. Antes de examinar la ICP que exige el documento núm. 9303 es necesario comprender cómo funcionan las firmas digitales.

30. El primer concepto importante se refiere a un par de claves criptográficas. Mediante la utilización de fórmulas matemáticas complejas, que dependen del algoritmo criptográfico específico que se esté empleando, se generan dos claves vinculadas. Cada clave consiste simplemente en un número aleatorio grande que se usa como parámetro en un algoritmo criptográfico específico; ambas claves tienen la propiedad de que lo que está encriptado en una sólo puede descifrarse con ayuda de la otra y viceversa. Una de las claves, la «clave privada», sólo es conocida por su propietario y no deberá revelarse a nadie; la otra, la «clave pública», es conocida y puede comunicarse a todo el mundo. Si el propietario de las claves encripta con la clave privada una secuencia de datos, por ejemplo las palabras «documento de identidad de la gente de mar», ésta se convierte en una secuencia aleatoria incoherente que no puede vincularse con el significado original. Ahora bien, cualquier persona que tenga una copia de la clave pública puede descifrar la secuencia y leer lo que esta decía originalmente. Sin embargo, la secuencia no podrá descifrarse y seguirá siendo incoherente si se usa la clave pública de otra persona.

31. El segundo concepto importante es el de condensación *(hash).* A una secuencia de datos de gran longitud, por ejemplo todos los contenidos de la zona de lectura mecánica de un pasaporte electrónico o de un DIM, puede aplicarse un algoritmo *hash* para producir una secuencia reducida denominada «compendio» *(hash digest).* Lo que caracteriza al compendio es que no puede utilizarse para determinar los datos originales, aunque

cualquier modificación de los datos originales alteraría considerablemente el compendio. Un ejemplo sencillo consistiría en tomar todos los caracteres de una secuencia y convertirlos a sus respectivos valores mediante el código ASCII (sistema normalizado de los Estados Unidos para el intercambio de información) (números comprendidos entre 0 y 255), sumarlos a continuación, dividirlos entre 100 y determinar el resto. Este procedimiento siempre daría como resultado un número comprendido entre 0 y 99, con independencia de la longitud de la secuencia original. A partir de un solo número comprendido entre 0 y 99 no podría calcularse la secuencia original, pero si se cambiara una sola letra de la secuencia el compendio también cambiaría. Es evidente que los algoritmos *hash* que se utilizan en la práctica son mucho más complejos, pero el principio es el mismo. Aunque resulta imposible calcular la secuencia original a partir del compendio, si se conoce la secuencia original es posible volver a generar un compendio.

32. Combinando estos dos conceptos puede crearse una firma digital. En el caso de un pasaporte electrónico o de un DIM, la autoridad expedidora genera un compendio de los datos que desea firmar (los contenidos de cada grupo de datos de la LDS del circuito integrado sin contacto). A continuación cifra este compendio utilizando la clave privada y almacena el compendio cifrado en el objeto de seguridad del documento (EF.SOD) del circuito integrado sin contacto. Al verificar la autenticidad del documento, las autoridades fronterizas u otras autoridades competentes leen en primer lugar el contenido de cada grupo de datos de la LDS y, después, el correspondiente compendio cifrado contenido en el objeto de seguridad del documento. A continuación generan su propia versión del compendio a partir de los datos que acaban de leer. Por último, para descifrar el compendio cifrado la autoridad verificadora utiliza la clave pública de la autoridad expedidora. Si el compendio descifrado coincide con el compendio generado por la autoridad que está verificando el documento, se tendrá la certeza de que:

a) los datos que se acaban de leer y utilizar para generar un compendio no han sido alterados y son exactamente los mismos que utilizó originalmente la autoridad expedidora para generar el compendio cifrado, y

b) la autoridad que expidió el documento es la misma que envió la clave pública a la autoridad fronteriza.

33. La ventaja de este sistema es que nadie puede firmar digitalmente un documento falso o fraudulento salvo si tiene acceso a una clave privada verdadera cuya clave pública haya sido distribuida a todas las autoridades verificadoras. Asimismo, una vez expedido y firmado digitalmente, el documento no podrá alterarse sin cambiar el compendio, lo que se detectará fácilmente al verificar la firma digital. Esto pone de relieve los dos puntos más importantes que deben tenerse presentes al expedir un documento protegido con firmas digitales:

a) la clave privada de la autoridad expedidora debe mantenerse en secreto y jamás deberá divulgarse a ninguna otra entidad;

b) debe haber un método seguro para que la autoridad expedidora facilite su clave pública a las autoridades verificadoras de todo el mundo, de modo que estas autoridades tengan la certeza de que esa clave pública procede de una autoridad expedidora lícita. Esto es lo que se denomina la infraestructura de clave pública o ICP.

34. Cabe señalar que la situación es más compleja de lo que se desprende de esta explicación básica. Cada clave se almacena en un certificado de formato normalizado y son estos certificados, no las claves, los que se intercambian. Existen asimismo distintos niveles de claves criptográficas, de manera que la clave privada utilizada para la firma de documentos en el momento de su expedición es siempre una clave provisional que cambia

periódicamente. La confianza en estas claves provisionales se basa en el hecho de que sus respectivos certificados se firman digitalmente mediante la utilización de una sola clave maestra, que en el ICP de la OACI (descrito en la parte 12 del documento núm. 9303) se asigna a la autoridad de certificación responsable de los certificados de firma electrónica (CSCA). La clave privada de la CSCA deberá protegerse muy escrupulosamente y solamente se utilizará para generar nuevos certificados cuando se modifiquen las claves provisionales (claves de firmante de documento). Existe un mecanismo para revocar certificados cuando la clave del firmante del documento ha sido comprometida, pero la clave de la CSCA debe manejarse con un nivel de seguridad tan elevado que ésta nunca quedaría expuesta. De ser el caso, se perdería la confianza en los documentos expedidos por el país de que se trate. Por regla general, las claves de la CSCA se cambian cada tres o cinco años, mientras que las claves de firmante de documento se cambian cada mes o cada tres meses.

35. La OACI administra su directorio de claves públicas (DCP) pero ha suscrito un contrato con una empresa privada para que se ocupe de su funcionamiento. Se trata de un sistema que permite distribuir en todo el mundo las claves públicas utilizadas para los pasaportes electrónicos, de modo que todos los organismos de control de fronteras, así como cualquier entidad que necesite verificar un pasaporte electrónico, puedan descargar una copia completa del DCP. Para acceder a este directorio por primera vez, la autoridad expedidora deberá disponer lo necesario para que uno de sus funcionarios se presente en persona en el centro de operaciones del DCP, donde se entrega y verifica el certificado inicial de la CSCA para registrarlo de manera segura en el DCP. Esta operación sirve para establecer la fiabilidad de las claves. Tras ello se recurre a mecanismos electrónicos para distribuir todos los certificados secundarios y las listas de revocación de certificados e incluso para cambiar el certificado de la CSCA, habida cuenta de que todas estas operaciones pueden verificarse utilizando el certificado inicial de la CSCA.

36. Si los anexos del Convenio núm. 185 se revisan según lo previsto, las autoridades competentes que quieran expedir los DIM de conformidad con lo dispuesto en los anexos revisados tendrán que prever un mecanismo plenamente compatible con la ICP descrita en la parte 12 del documento núm. 9303 a efectos de firmar digitalmente los contenidos de la LDS en el circuito integrado sin contacto. Ello significa que las claves públicas tendrían que distribuirse a todas las autoridades fronterizas y ponerse a disposición de las demás entidades que necesiten autenticar los DIM. Al mismo tiempo, las claves privadas deberían protegerse escrupulosamente, de modo que la confianza en los certificados utilizados para firmar los DIM sea equivalente a la confianza en los certificados utilizados para firmar los pasaportes electrónicos.

37. Aunque en teoría sería posible que una autoridad expedidora de DIM estableciera su propia infraestructura de clave pública para dar cumplimiento a los requisitos indicados, las dificultades que en la práctica se han planteado para convencer a las autoridades fronterizas de que utilicen el DCP sugieren que sería muy difícil convencerlas de que utilicen otro mecanismo equivalente exclusivamente para los DIM ya que, en comparación con el número de pasaportes electrónicos, el número de DIM que las autoridades fronterizas tienen oportunidad de ver es extremadamente reducido. Así pues, en el caso de los DIM expedidos de conformidad con lo dispuesto en los anexos revisados del Convenio núm. 185 propuestos, la única solución práctica sería utilizar como ICP el directorio de claves públicas.

38. La plena participación en el DCP es muy costosa: para 2015, la cuota inicial ha sido fijada en 56 000 dólares de los Estados Unidos, y la cuota anual en 43 642 dólares.

39. Es posible que se produzcan confusiones si la autoridad expedidora de pasaportes electrónicos y la autoridad responsable de la expedición de los DIM del mismo país cuentan cada una con su propia CSCA. Aunque en teoría esto es posible en el marco del

DCP, puesto que varios países tienen más de una autoridad expedidora de pasaportes electrónicos, no es sin embargo la forma en que normalmente funciona el directorio.

40. La autoridad expedidora de DIM podrá registrar sus certificados en el directorio incluso en el caso de que no participe en el DCP. Para ello, otra entidad participante en el DCP deberá prestarse a firmar digitalmente e incluir en su lista maestra el certificado de la CSCA de la autoridad expedidora.

41. En conclusión, existen muchos mecanismos que la autoridad expedidora de DIM podría utilizar para aplicar los requisitos relativos a la ICP indicados en el documento núm. 9303. La solución escogida dependerá de cada Miembro de la OIT que ratifique el Convenio núm. 185. Ahora bien, lo más simple sería recomendar una misma solución para todos los Miembros. Convendría contar con orientaciones a este respecto, y por eso se pedirá a la OACI que proporcione orientaciones sobre el particular en la reunión del Comité Marítimo Tripartito *ad hoc* en la que se examinará el proyecto preliminar que figura en la parte I del presente documento.

III. De qué modo podría gestionarse un sistema de expedición con arreglo a los anexos enmendados

42. Las explicaciones que preceden sobre los importantes cambios en el DIM y en el proceso de expedición del DIM ponen de manifiesto que la aplicación de los anexos sería sin duda más compleja y costosa si éstos se enmendaran tal como se propone en el proyecto preliminar. En virtud de los anexos, tal como están redactados actualmente, todas las autoridades que expiden DIM de conformidad con el Convenio núm. 185 siguen el mismo proceso básico. El proceso actual puede dividirse en los pasos siguientes:

a) Se obtienen y se registran los datos personales del solicitante de un DIM, así como una fotografía de éste y sus huellas dactilares.

b) Se examinan los documentos del solicitante con objeto de comprobar su identidad y su nacionalidad o lugar de residencia, además de verificar su condición de marino.

c) Toda la información acerca del solicitante y de la solicitud de DIM se registra y se transfiere a un funcionario de la autoridad expedidora de DIM distinto del que recibió la solicitud y registró los datos. Ese segundo funcionario debe verificar la solicitud y autorizar la producción del DIM.

d) Se efectúan varias comprobaciones de seguridad. Éstas pueden consistir en verificaciones en las bases de datos de la policía local o en escuelas navales o empresas navieras a fin de comprobar que el solicitante es, efectivamente, un marino. Las comprobaciones específicas pueden variar.

e) Una vez que se han llevado a cabo satisfactoriamente las comprobaciones de seguridad y se ha recibido la autorización, se imprime el DIM, con el código de barras bidimensional en el que se almacenan las huellas dactilares.

f) Se comprueba el DIM impreso para asegurarse de que los datos son correctos y de que todos los elementos se han impreso adecuadamente y son legibles. Este paso se conoce como aseguramiento de la calidad y, si bien se recomienda que se lleve a cabo en todos los DIM, puede efectuarse de forma aleatoria. Si se detecta alguna anomalía, deberán repetirse los pasos *e)* y *f).*

g) Se crea una entrada en la base electrónica de datos nacional para el DIM que acaba de imprimirse.

h) Se expide el DIM al marino.

43. Todos estos trámites pueden realizarse en el mismo lugar, pero también es posible disponer de varios centros de inscripción en los que se lleven a cabo los pasos *a), b)* e incluso *h),* mientras que los demás trámites se realizarían en la oficina central.

44. Si se revisan los anexos del Convenio núm. 185 con arreglo a las propuestas contenidas en el proyecto preliminar, el nuevo proceso será más complejo y conllevará los pasos siguientes:

a) Se obtienen y se registran los datos personales del solicitante de un DIM, así como una fotografía de éste.

b) Se examinan los documentos del solicitante con objeto de comprobar su identidad y su nacionalidad o lugar de residencia, además de verificar su condición de marino.

c) Toda la información acerca del solicitante y de la solicitud de DIM se registra y se transfiere a un funcionario de la autoridad expedidora de DIM distinto del que recibió la solicitud y registró los datos. Ese segundo funcionario debe verificar la solicitud y autorizar la producción del DIM.

d) Se efectúan varias comprobaciones de seguridad. Estas pueden consistir en verificaciones en las bases de datos de la policía local o en escuelas navales o empresas navieras a fin de comprobar que el solicitante es, efectivamente, un marino. Las comprobaciones específicas pueden variar.

e) Una vez que se han llevado a cabo satisfactoriamente las comprobaciones de seguridad y se ha recibido la autorización, se imprime el DIM.

f) Se formatean y se firman digitalmente los datos que se han de almacenar en el circuito integrado sin contacto.

g) Se escriben los datos en el circuito integrado sin contacto, el cual se protege contra escritura para que no sea posible introducir en él más datos.

h) Se comprueba el DIM impreso para asegurarse de que los datos son correctos y de que todos los elementos se han impreso correctamente y son legibles.

i) Se comprueba el contenido del circuito integrado sin contacto a fin de asegurarse de que se ha codificado correctamente, y en particular que su contenido se corresponde con los datos impresos y que las firmas digitales pueden validarse correctamente mediante la clave pública correspondiente. Si se detecta alguna anomalía, deberán repetirse los pasos *e)* a *i).*

j) Se crea una entrada en la base electrónica de datos nacional para el DIM que acaba de imprimirse.

k) Se expide el DIM al marino.

l) Las claves públicas necesarias para verificar la autenticidad del DIM se distribuyen de manera segura a todas las autoridades que puedan necesitarlas para comprobar los DIM. Este paso sólo será necesario cuando se cambie una clave (con una frecuencia de entre uno y tres meses en el caso de las claves del firmante del documento).

45. También en este caso, aunque todos los trámites pueden realizarse en el mismo lugar, es posible, asimismo, llevarlos a cabo en distintos lugares por razones prácticas.

46. No compete al Comité Marítimo Tripartito facilitar asesoramiento o tomar decisiones respecto de las modalidades de expedición de DIM con arreglo a los anexos revisados del Convenio núm. 185 propuestos. No obstante, a continuación se presentan tres posibles opciones a ese respecto, de modo que el Comité pueda evaluar en qué medida los Miembros de la OIT podrían hacer frente, desde un punto de vista económico y de manera realista, a la complejidad adicional que supondría la introducción de un sistema de circuito integrado sin contacto con firmas digitales y la ICP conexa.

A. Producción de los DIM por la propia autoridad expedidora de DIM

47. Esta sería la opción predeterminada. La autoridad expedidora de DIM se encargaría de todos los pasos del proceso enumerados en el párrafo 44 del presente documento. En ese caso, sería necesario que el Miembro sufragara el costo de la participación plena en el DCP

o, si fuera posible, que encontrara otra entidad participante en ese directorio que se prestara a incluir los certificados de los DIM en su lista maestra.

48. Se trata de la opción más cara, en especial si fuera necesario que la autoridad expedidora de DIM participara a título propio en el DCP. También sería la más compleja desde un punto de vista técnico. El inconveniente es que el hecho de añadir autoridades expedidoras de DIM al DCP podría representar un riesgo para la seguridad. Esto se debe a que las claves utilizadas para firmar digitalmente los DIM también podrían emplearse para firmar pasaportes electrónicos y, si esas claves formaran parte del DCP, prácticamente ningún sistema de inspección en los puestos fronterizos podría determinar si las claves se están utilizando legítimamente. Así pues, existiría la posibilidad de que una clave comprometida utilizada por una autoridad expedidora de DIM pudiera emplearse para elaborar pasaportes electrónicos fraudulentos. Además, es posible que se considere que las autoridades expedidoras de DIM son menos capaces de gestionar de manera segura sus claves e impedir su uso con fines fraudulentos que las autoridades expedidoras de pasaportes electrónicos. Por consiguiente, sería importante que todas las autoridades expedidoras de DIM demostraran claramente su capacidad y comprensión de los protocolos de seguridad adecuados, de manera que se les permitiera participar en el DCP.

49. Con todo, esa opción ofrecería varias ventajas. Permitiría que la autoridad expedidora de DIM gestionara todos los aspectos del proceso de expedición y velara por que sus protocolos de seguridad se aplicaran en todo el proceso. Además, los programas y equipos informáticos de expedición se podrían diseñar y fabricar como un sistema unificado con el objetivo específico de expedir DIM. De este modo, se dispondría de un sistema eficiente y eficaz con el que sería posible atender todos los aspectos propios de la expedición de un DIM con arreglo a lo dispuesto en el Convenio núm. 185, frente a la expedición de un pasaporte electrónico u otro tipo de documentos.

50. Las desventajas serían su costo (especialmente la participación en el DCP) y la complejidad que para la autoridad expedidora de DIM entrañaría la adquisición de conocimientos sobre las nuevas tecnologías (circuitos integrados sin contacto, firmas digitales e ICP).

B. Producción de los DIM por la autoridad expedidora de pasaportes electrónicos

51. Una de las soluciones más sencillas para una autoridad que expide DIM con arreglo a los anexos revisados del Convenio núm. 185 propuestos sería delegar todo el proceso de expedición en su autoridad nacional expedidora de pasaportes electrónicos. Si el Miembro de la OIT ya expide pasaportes electrónicos y participa en el DCP, su autoridad nacional expedidora de pasaportes electrónicos ya se habrá dotado de infraestructura para gestionar circuitos integrados sin contacto y contará con todos los programas y equipos informáticos necesarios para su codificación. En ese caso, se encargaría a la autoridad expedidora de pasaportes electrónicos la realización de los pasos *a)* a *l)* enumerados en el párrafo 44 del presente documento. La gestión de la base electrónica de datos nacional y del centro permanente de coordinación correspondiente podría correr a cargo de la autoridad expedidora de DIM o de la autoridad expedidora de pasaportes electrónicos.

52. La principal ventaja que ofrece esta opción es que la compleja labor de gestionar las firmas digitales, los certificados y la ICP estaría a cargo de una entidad que ya ha invertido en la infraestructura necesaria para su gestión. Habida cuenta de que podría utilizarse la misma CSCA para firmar todos los documentos expedidos por la misma autoridad encargada de la expedición de pasaportes electrónicos, la gestión de la ICP no entrañaría ningún costo extraordinario ni requeriría ningún esfuerzo adicional, lo que supondría un ahorro considerable para el Estado Miembro.

53. Aun así, la autoridad expedidora de pasaportes electrónicos tendría que dotarse de impresoras capaces de imprimir un documento del tamaño de una tarjeta de crédito en lugar de una libreta de pasaporte y modificar sus programas informáticos de expedición para poder tramitar DIM; en todo caso, se mantendría la mayoría de las características de los programas informáticos y del proceso de expedición actuales. El costo de esas modificaciones sería muy inferior al costo de desarrollar un sistema de expedición completamente nuevo.

54. El posible inconveniente de esta opción sería la pérdida de control por la autoridad expedidora de DIM, ya que delegaría sus cometidos en otra autoridad del mismo país. Puede que las dos autoridades expedidoras también tuvieran dificultades para coordinarse. Cabe la posibilidad de que muchas autoridades expedidoras de pasaportes electrónicos no deseen modificar sus programas informáticos ni dotarse de medios de impresión adicionales para un documento de otro tamaño.

55. Podrían plantearse problemas por no entender el personal de la autoridad expedidora de pasaportes electrónicos cómo se comprueba correctamente la documentación de un marino. Aunque probablemente ese personal esté familiarizado con las comprobaciones de la identidad, nacionalidad o lugar de residencia, la verificación de que el solicitante es un marino no es algo que el personal encargado de la expedición de pasaportes acostumbre hacer. Con todo, podría subsanarse esa dificultad por medio de un sistema híbrido en el que la autoridad expedidora de DIM realizara los pasos *a)*, *b)* e incluso *c)* y *k)* y la autoridad expedidora de pasaportes electrónicos se ocupara de los restantes pasos.

56. En resumen, esta opción sería rentable y segura, pero su aplicación exigiría una buena cooperación a nivel interno.

C. Inscripción del marino por la autoridad expedidora de DIM y externalización de la producción de los DIM

57. Con esta opción, la autoridad expedidora de DIM conservaría el control del proceso de expedición, pero externalizaría partes de ese proceso a una entidad jurídica independiente, con lo que se evitaría una parte de los costos y la complejidad mencionados. Los Miembros de la OIT ratificantes que estuvieran interesados en esta opción podrían concertarse con esa entidad. La entidad independiente estaría al margen del control de los Miembros de la OIT, ya que ofrecería sus servicios a varias autoridades nacionales expedidoras de DIM. A los fines de la presente explicación, se denominará a esa entidad independiente «oficina central de tramitación» (OCT).

58. En este caso, la autoridad expedidora de DIM llevaría a cabo los pasos *a)* a *d)* indicados en el párrafo 44 del presente documento, pero, en lugar de utilizar su propio programa informático de expedición, emplearía una aplicación en línea alojada en servidores centrales. Esos servidores estarían alojados en la OCT, pero la base de datos de cada una de las autoridades expedidoras se mantendría separada de las demás y su contenido sería confidencial. La OCT realizaría los pasos *e)* a *j)* y *l)* en nombre de la autoridad expedidora de DIM. Del paso *k)* (expedición del DIM) podría encargarse directamente la OCT mediante el envío directo del DIM acabado al marino, si bien sería preferible que la OCT enviase el DIM acabado a la autoridad expedidora de DIM para que esta procediese a su entrega.

59. La autoridad expedidora seguirá siendo el único órgano competente responsable de la inscripción del marino, inclusive en lo relativo a la obtención de sus datos personales y su fotografía y la verificación de su identidad, nacionalidad o lugar de residencia, así como de su condición de marino, ya que, de conformidad con lo dispuesto en el Convenio, esa responsabilidad corresponderá al Estado de la nacionalidad del marino o de su residencia

permanente, que es la autoridad más capacitada para llevar a cabo las comprobaciones necesarias. De manera análoga, las comprobaciones de seguridad y la decisión final de autorizar la impresión de un DIM seguirán siendo competencia de la autoridad expedidora. En cambio, la responsabilidad respecto de la impresión del DIM, la codificación del circuito integrado sin contacto y la gestión de la ICP se delegaría en la OCT.

60. La ventaja de esta opción reside en que la OCT solo tendría que desarrollar un único conjunto de programas informáticos de expedición y disponer de un único equipo informático de impresión y codificación de circuitos integrados, independientemente del número de Miembros de la OIT que decidan utilizar sus servicios. Evidentemente, sería necesario que hubiera más servidores y más impresoras a medida que el volumen de actividad aumentara, pero el número total de DIM que se expedirían a escala mundial en un año sería bastante reducido (entre 400 000 y 600 000), incluso en el caso de que la mayoría de los Estados Miembros de la OIT ratificase el Convenio y decidiese recurrir a la OCT. Esa cifra se aproximaría al número de pasaportes electrónicos expedidos anualmente por un país de tamaño mediano. Con ello disminuiría la necesidad de que cada uno de los Miembros de la OIT sufragara todos los gastos de desarrollo de un sistema de expedición y de gestión de la ICP, tal como sucede en el caso de los pasaportes electrónicos. También es probable que pudiera usarse una única autoridad CSCA para identificar todos los DIM expedidos por la OCT para todos los Miembros de la OIT, empleándose claves del firmante de documentos separadas para cada uno de los Miembros. Todo ello simplificaría considerablemente la gestión de la ICP.

61. Si escogiese esta opción, la autoridad expedidora de DIM necesitaría disponer de computadoras conectadas a Internet y cámaras o escáneres que permitieran captar la imagen del rostro del marino, pero no sería necesario que contara con una impresora ni con un equipo informático para la codificación de circuitos integrados, ni tampoco con su propio programa informático de expedición. Estos últimos elementos estarían ubicados en la OCT. Sería necesario que la autoridad expedidora de DIM tuviera por lo menos un lector de pasaportes electrónicos, de manera que los datos de los DIM pudieran ser leídos y mostrados a los marinos que desearan ejercer su derecho a examinar todos aquellos datos que se refieran a ellos y no puedan leerse a simple vista, en virtud de lo dispuesto en el párrafo 9 del artículo 3 del Convenio núm. 185. Con ello se lograría un ahorro muy sustancioso en equipos y programas informáticos.

62. La autoridad expedidora de DIM conservaría el control de los datos relacionados con sus marinos, ya que los servidores centrales estarían alojados en instalaciones seguras y los datos de cada una de las autoridades expedidoras se consignarían por separado y sólo serían accesibles para el personal de esa autoridad y, únicamente con fines de impresión, para el personal de la OCT. Todas las comprobaciones de seguridad habituales podrían llevarse a cabo en el territorio del Estado Miembro y la decisión de autorizar la expedición de un DIM seguiría estando en manos de un funcionario de la autoridad expedidora de DIM; no obstante, el registro de la decisión de autorizar esa expedición se almacenaría en los servidores centrales de la OCT.

63. Por consiguiente, el costo de expedir los DIM con arreglo a lo dispuesto en los anexos revisados del Convenio núm. 185 propuestos disminuiría ostensiblemente, puesto que la mayoría de los gastos de infraestructura se repartirían entre los Miembros que decidieran utilizar la OCT. No disminuiría el nivel de seguridad; es más, probablemente aumentaría si se eligiera una OCT fiable, ya que la impresión y la codificación de los DIM se realizarían en instalaciones seguras cuyo personal tendría pocas probabilidades de colaborar con los funcionarios de la autoridad expedidora de DIM en expediciones fraudulentas, dada su lejanía geográfica. También se simplificaría la gestión de la ICP, sobre todo si la OCT utilizara una única CSCA para todos los DIM.

64. Una de las desventajas de esta opción sería que las autoridades expedidoras de DIM perderían la posibilidad de adaptar el funcionamiento de su sistema de expedición. Todos aquellos que recurrieran a la OCT tendrían que utilizar el mismo sistema de expedición, con los mismos protocolos y la misma interfaz de usuario. Probablemente habría suficiente flexibilidad para permitir pequeñas variaciones en el diseño de los DIM impresos como, por ejemplo, las banderas nacionales, pero la mayoría de los elementos tendrían que ser los mismos en todos los DIM o, de lo contrario, se perdería buena parte de los beneficios en materia de costos.

65. Otra desventaja es que se desalentaría el establecimiento de todo vínculo automatizado entre el sistema de expedición de DIM y otros sistemas que pudieran utilizarse para realizar comprobaciones de seguridad (por ejemplo, un sistema nacional de policía o una base de datos de las escuelas navales), puesto que se necesitaría la adición de módulos específicos para cada país a los programas informáticos de expedición de la OCT. Aunque no se sabe a ciencia cierta si algún Miembro de la OIT ha establecido esos vínculos automatizados en el marco de las comprobaciones de seguridad en alguno de los sistemas de expedición de DIM existentes, es importante señalar que esos vínculos exigirían un esfuerzo adicional y, por tanto, también acarrearían un costo adicional.

66. Sin embargo, la principal desventaja que presenta esta opción es que podría resultar difícil encontrar una entidad dispuesta a actuar como OCT. Esto se debe a que la tasa de ratificación del Convenio núm. 185 y, especialmente, la tasa de expedición de DIM progresan con lentitud y la OCT tendría dificultades para estimar cuántos Miembros de la OIT podrían decidir utilizar sus servicios y en qué plazo lo harían. Dado que la principal ventaja de la presente opción reside en que el costo del equipo y los programas informáticos y de la gestión de la ICP se dividiría entre todos los países que utilizaran la OCT, el ahorro sería directamente proporcional al número de autoridades expedidoras de DIM que decidieran recurrir a la OCT. Este problema es similar al que se plantea respecto del DCP, cuya cuota de participación tiende a disminuir cada año a medida que aumenta el número de países participantes. Este efecto se vería multiplicado en el caso de la OCT, puesto que no sólo gestionaría una ICP, sino todo el sistema de producción y expedición de documentos.

67. La forma más realista de resolver esa cuestión sería que la OIT se coordinara con varios Miembros interesados hasta que hubiera un número suficiente que justificara el gasto de establecer la OCT. Se podría abrir entonces un proceso de licitación, dirigido por la OIT o por uno de los Miembros, con objeto de encontrar una entidad dispuesta a establecer y gestionar la OCT. El costo inicial dependería del número de Miembros que participaran en un principio, y se alcanzaría un acuerdo para rebajar la cuota a medida que se alcanzasen determinados umbrales, consistentes en el número de Miembros participantes y el número de DIM expedidos anualmente.

68. De hecho, la impresión de documentos seguros en una imprenta compartida es una práctica bastante extendida. Así ocurre en el caso de muchas solicitudes de distinto tipo, y un número muy considerable de países incluso subcontrata la impresión de sellos y papel moneda a alguna de las principales imprentas de seguridad del mercado internacional.

69. La utilización de un sistema de expedición compartido por varios países es menos común, pero no deja de ser un aspecto más de la nueva tendencia consistente en trasladar a la nube tantos procesos informáticos como sea posible. Actualmente, muchas empresas privadas y numerosos gobiernos utilizan la computación en nube alojada en servidores centrales y, por lo que parece, su popularidad no deja de aumentar. En 2015, se registró el primer caso de impresión en nube de pasaportes electrónicos cuando seis territorios del Reino Unido comenzaron a expedir pasaportes electrónicos por medio de un sistema en nube único y compartido.

70. Otro enfoque que podría adoptarse una vez creada la OCT consistiría en que las autoridades expedidoras de DIM permitieran que la OCT gestionara su base electrónica de datos nacional y prestara apoyo a su centro permanente de coordinación. Como los datos seguirían estando controlados por la autoridad expedidora de DIM (aunque se almacenarían en un centro de datos seguro gestionado por la OCT), sería lógico que la OCT prestara servicio las 24 horas del día, tal como requieren los centros permanentes de coordinación, y colocara una parte de los datos que almacena, necesarios para el proceso de expedición de los DIM, en una base electrónica de datos nacional propia de cada una de las autoridades expedidoras participantes, a la cual podría tener acceso el centro permanente de coordinación correspondiente. Todo ello podría redundar en un ahorro de recursos financieros, ya que garantizar la disponibilidad de un centro de coordinación que preste servicio las 24 horas del día, tal como se estipula en el párrafo 4 del artículo 4 del Convenio núm. 185, es caro. Además, facilitaría la labor de las autoridades fronterizas y de otras entidades que desearan verificar un DIM por conducto de los centros permanentes de coordinación, puesto que podrían utilizar los mismos datos de contacto (número de teléfono, dirección de correo electrónico, URL, etc.) para todos los Miembros de la OIT que hubieran decidido subcontratar esas tareas a la OCT.

71. En resumen, esta opción podría suponer un ahorro de recursos financieros y consistiría en subcontratar los nuevos elementos complejos relacionados con el uso de un circuito integrado sin contacto en el DIM y la gestión de las firmas digitales y del DCP a un tercero con conocimientos especializados en esos campos. Además, ofrecería la posibilidad de simplificar la gestión de la base electrónica de datos nacional y del centro permanente de coordinación. Aunque esta opción requeriría que los Miembros de la OIT interesados se coordinaran para lograr que su implantación fuera rentable, esa rentabilidad aumentaría a medida que participaran más Miembros.

IV. Addéndum

Observaciones de la Organización de Aviación Civil Internacional (OACI)

72. El 8 de enero de 2016 la Oficina Internacional del Trabajo recibió las observaciones de la Organización de Aviación Civil Internacional (OACI) a los *Comentarios y propuestas de enmienda de los anexos I, II y III del Convenio núm. 185* contenidos en el documento de referencia que se preparó para la reunión del Comité Tripartito Marítimo *ad hoc*. Estas observaciones se refieren principalmente a la firma digital de los documentos de identidad de la gente de mar (DIM) al aplicar las enmiendas propuestas. Las consecuencias de la introducción de dichas enmiendas para las tres opciones que se presentan en la parte III del documento de referencia podrían resumirse de la siguiente manera:

- Opción A: Producción de los DIM por la propia autoridad expedidora de DIM (párrafos 47 a 50 del documento de referencia). Esta opción no sería viable para la OACI a menos que la autoridad expedidora de DIM colaborase con la autoridad expedidora de pasaportes electrónicos para la obtención de claves de la autoridad de certificación responsable de los certificados de firma electrónica (CSCA), y la propietaria de las claves fuera la autoridad expedidora de pasaportes electrónicos.

- Opción B: Producción de los DIM por la autoridad expedidora de pasaportes electrónicos (párrafos 51 a 56 del documento de referencia). La OACI es favorable a la opción B tanto en el caso de que la autoridad expedidora de pasaportes electrónicos se encargara de todos los pasos del proceso de expedición de documentos como en el caso de que la autoridad expedidora de pasaportes electrónicos y la autoridad expedidora de DIM tuvieran que compartir la responsabilidad de las distintas etapas

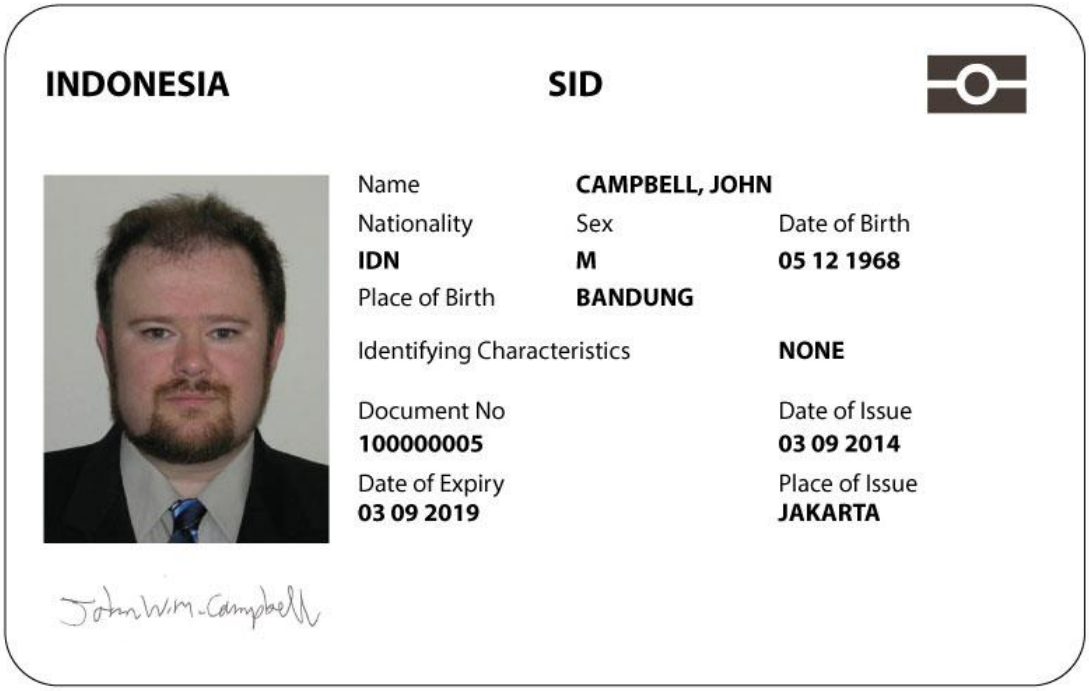
del proceso, siempre que se utilice la infraestructura existente en el país para la firma de pasaportes electrónicos.

- Opción C: Inscripción del marino por la autoridad expedidora de DIM y externalización de la producción de los DIM (párrafos 57 a 71 del documento de referencia). Para la OACI, esta opción sólo sería posible en caso de que la OIT tuviera el control de la oficina central de tramitación (OCT) y colaborase con la autoridad expedidora de *laissez-passer* de las Naciones Unidas para utilizar su CSCA. La OACI considera que esta opción también podría aplicarse conjuntamente con las opciones anteriores.

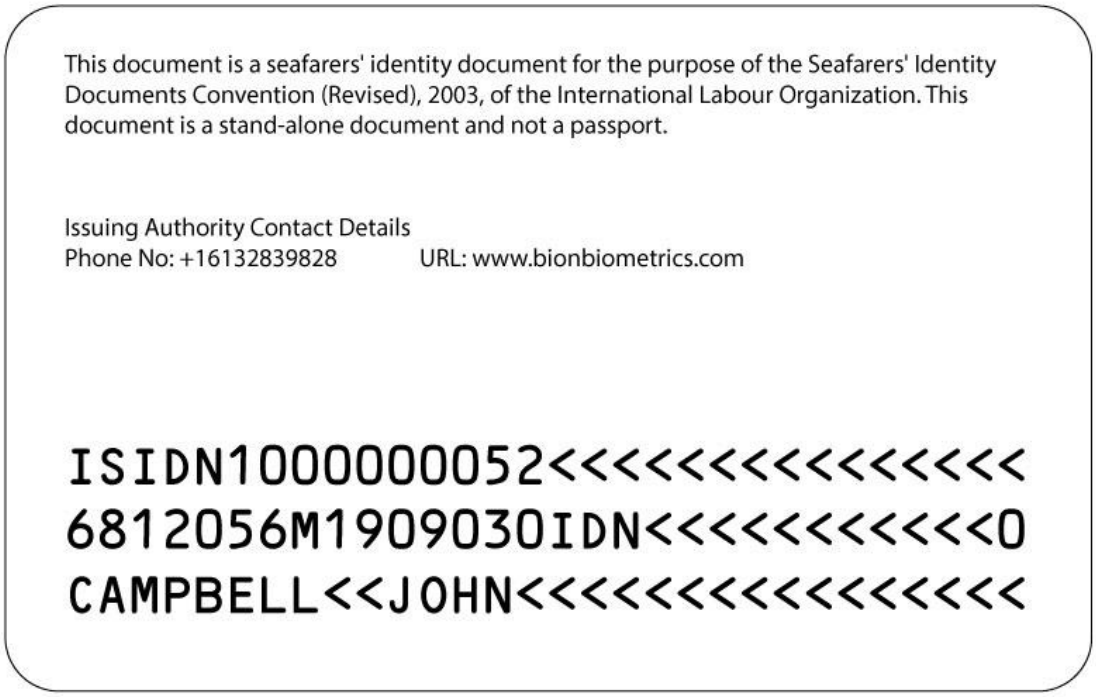
73. El Comité Marítimo Tripartito *ad hoc* tal vez estime oportuno tomar nota de que la opción C, según se refleja en las observaciones de la OACI, requeriría un examen minucioso del papel y las responsabilidades de la OIT, inclusive de las repercusiones financieras, y tendría que ser objeto de amplias consultas con las Naciones Unidas.

Anexo

Ejemplo de documento de identidad de la gente de mar elaborado según la propuesta de versión enmendada del anexo I del Convenio núm. 185



Anverso



Reverso

INDONESIA	DIM	
Nombre	CAMPBELL, JOHN	
Nacionalidad	Sexo	Fecha de nacimiento
IDN	M	05 12 1968
Lugar de nacimiento	BANDUNG	
Características identificativas		NINGUNA
Núm. de documento 100000005		Fecha de expedición 03 09 2014
Fecha de caducidad		Lugar de expedición
03 09 2019		YAKARTA

Este es un documento de identidad de la gente de mar a los efectos del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003, de la Organización Internacional del Trabajo. Este documento es autónomo, y no es un pasaporte

Datos de contacto de la autoridad expedidora:
Núm. de teléfono: + 161 328 398 28 URL: www.bionbiometrics.com