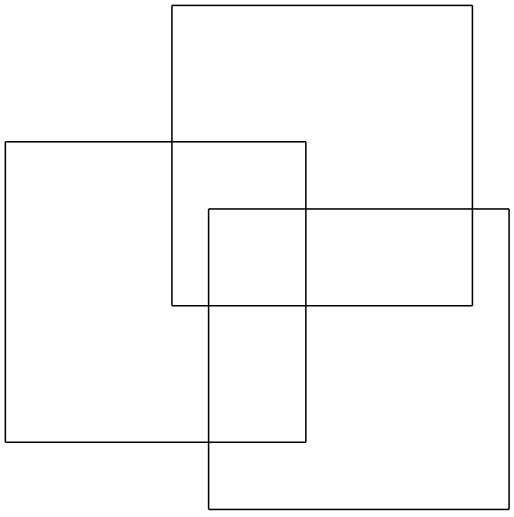
MESIDC/2015

Oficina
Internacional
del Trabajo

Ginebra

Documento técnico de referencia para la discusión en la reunión de expertos sobre el Convenio núm. 185
(Ginebra, 4-6 de febrero de 2015)



Departamento
de Normas
Internacionales
del Trabajo

Departamento
de Políticas
Sectoriales

Ginebra, 2015

MESIDC/2015

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO

Departamento de Normas Internacionales del Trabajo
Departamento de Políticas Sectoriales

Documento técnico de referencia para la discusión en la reunión de expertos sobre el Convenio núm. 185
(Ginebra, 4-6 de febrero de 2015)

Ginebra, 2015

OFICINA INTERNACIONAL DEL TRABAJO, GINEBRA

Primera edición 2015

Documento técnico de referencia para la discusión en la reunión de expertos sobre el Convenio núm. 185 (Ginebra, 4-6 de febrero de 2015)/Departamento de Normas Internacionales del Trabajo y Departamento de Políticas Sectoriales, Ginebra, OIT, 2014.

ISBN: 978-92-2-329369-7 (impreso)
ISBN: 978-92-2-329370-3 (web pdf)

Impreso por la Oficina Internacional del Trabajo, Ginebra, Suiza

Índice

Página

I. Introducción 1

II. Contexto 2

A. La situación actual del Convenio núm. 185 2

B. Breve resumen del Convenio núm. 185 y medidas para apoyar su aplicación 3

III. Opciones a examinar en relación con la aplicación del Convenio núm. 185 7

A. Opciones para los Miembros que han ratificado el Convenio núm. 185 o tienen previsto hacerlo en relación con el contenido y la expedición de los DIM 9

A-1. Actualizaciones menores del contenido de los DIM a fin de reflejar las normas más recientes 9

A-2. Respaldar la continua compatibilidad de las huellas dactilares 12

A-3. Incorporación de una firma digital al código de barras de los DIM 14

A-4. Elaboración de DIM que funcionen con chips 17

A-5. Cambiar los datos biométricos, a saber cambiar la huella digital de un código de barras por una imagen facial 19

A-6. Establecimiento de una entidad de coordinación de centros de coordinación 22

A-7. Colaboración entre los Miembros para establecer sistemas de expedición de DIM 26

B. Opciones para los Miembros que no han ratificado el Convenio núm. 185 en relación con el uso de DIM expedidos en virtud de dicho Convenio 27

B-1. Usar los DIM expedidos en virtud del Convenio núm. 185 para tomar decisiones en relación con la admisión de marinos 28

B-2. Verificar la identidad de los marinos 30

B-3. Autentificar los DIM 30

Anexos

I. Ratificaciones del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185) (al 30 de noviembre de 2014) 33

II. Partes seleccionadas de la norma ISO/IEC 24713-3:2009 34

I. Introducción

1. En su 320.ª reunión (marzo de 2014), el Consejo de Administración de la Oficina Internacional del Trabajo, tras un examen inicial del documento titulado «Cooperación internacional en relación con el Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185)» [1], consideró que debido a la compleja cuestión técnica que se plantea en este documento, tanto sobre cuestiones marítimas como sobre cuestiones de control fronterizo y visados, sería importante obtener el asesoramiento de expertos sobre la viabilidad, los costos y los beneficios de diversas soluciones técnicas y de otra índole. Este asesoramiento ayudaría al Consejo de Administración a tomar una decisión sobre el mejor enfoque para avanzar hacia el logro de los objetivos del Convenio.

2. Los Miembros del Consejo de Administración señalaron la importancia de estas cuestiones tanto para los armadores como para la gente de mar y la necesidad de avanzar. Por consiguiente, el Consejo de Administración tomó la siguiente decisión inicial:

a) celebrar una reunión en la que participaran expertos marítimos y expertos en visados, dentro de los recursos disponibles, con objeto de examinar la viabilidad y realizar un análisis de los costos y beneficios de las diversas opciones contempladas — incluidas las definidas en el documento GB.320/LILS/5 — para solucionar las dificultades que plantea la aplicación del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185) a los Estados del pabellón, los Estados del puerto y los Estados que suministran a la gente de mar ratificantes y no ratificantes, así como a los armadores y la gente de mar, y

b) examinar los resultados de tal reunión en una futura reunión del Consejo de Administración.

3. En su 321.ª reunión (junio de 2014), el Consejo de Administración tomó otras decisiones en relación con la composición de esta reunión tripartita de expertos [2].

4. Este documento de referencia tiene por objeto ofrecer información a fin de facilitar los debates en la reunión tripartita de expertos y está organizado en tres partes, a saber esta primera parte y dos anexos. En el capítulo II de esta primera parte se proporciona información sobre la situación actual del Convenio núm. 185 y sus antecedentes, así como sobre sus objetivos y los problemas actuales. En el capítulo III se examinan las opciones, incluidas las consideraciones en materia de costes y beneficios, en lo que respecta a la aplicación del Convenio y el logro de sus objetivos. Esas opciones se exponen en dos secciones, A y B, teniendo en cuenta las dos diferentes situaciones de los Miembros. En la sección A se examinan los problemas y las posibles soluciones en relación con los Miembros de la Organización Internacional del Trabajo (OIT) que han ratificado el Convenio núm. 185 y, en la mayor parte de los casos, han realizado importantes inversiones en tecnología para aplicarlo. En la sección B se examinan las cuestiones y las posibles opciones en relación con los Miembros que no han ratificado el Convenio núm. 185 pero pueden tener intereses en el ámbito marítimo, incluidas las cuestiones relacionadas con el bienestar de la gente de mar, la viabilidad del transporte marítimo internacional y la seguridad. A este respecto también se señala que, en virtud del artículo 19 de la Constitución de la OIT, aunque un Miembro no esté obligado por un convenio tiene la obligación subyacente de informar, con la frecuencia apropiada, al Director

[1] Documento GB.320/LILS/5.

[2] Documento GB.321/INS/11, párrafos 3-6.

General de la OIT sobre el estado de su legislación y su práctica en lo que respecta a los asuntos tratados en ese convenio, precisando en qué medida se ha puesto o se propone poner en ejecución cualquiera de sus disposiciones, por vía legislativa o administrativa, por medio de contratos colectivos, o de otro modo, e indicando las dificultades que impiden o retrasan su ratificación.

II. Contexto

A. La situación actual del Convenio núm. 185

5. El Convenio núm. 185 se adoptó en 2003 para sustituir el Convenio sobre los documentos de identidad de la gente de mar, 1958 (núm. 108), que, aunque había sido ampliamente ratificado, contenía disposiciones en materia de seguridad que habían perdido vigencia. La OIT siguió un procedimiento acelerado [3] para la rápida adopción y aplicación del Convenio a fin de atender eficazmente las necesidades de seguridad reforzada que surgieron tras el 11 de septiembre de 2001. Además, posteriormente se decidió no incluir este tema en el Convenio sobre el trabajo marítimo, 2006 (MLC, 2006), que refunde la mayor parte de los convenios (37) y recomendaciones (31) sobre el trabajo marítimo existentes, e incluye un procedimiento que permite modificaciones más rápidas a fin de velar por que las exigencias técnicas puedan responder a las necesidades cambiantes del sector.

6. El Convenio núm. 185 entró en vigor el 9 de febrero de 2005 y lo han ratificado (o aplican provisionalmente) [4] 28 países: Albania, Azerbaiyán, Bahamas, Bangladesh, Bosnia y Herzegovina, Brasil, Congo, República de Corea, Croacia, España, Filipinas, Francia, Hungría, Indonesia, Islas Marshall, Jordania, Kazajstán, Kiribati, Lituania, Luxemburgo, Madagascar, República de Moldova, Nigeria, Pakistán, Federación de Rusia, Turkmenistán, Vanuatu y Yemen (véase el anexo 1 para más detalles).

[3] Tras las discusiones preliminares en la Organización Marítima Internacional (OMI) sobre la mejora de las medidas de seguridad aplicables al sector marítimo, en la 283.ª reunión (marzo de 2002) del Consejo de Administración se decidió inscribir en el orden del día de la 91.ª reunión de la Conferencia Internacional del Trabajo (2003) un punto sobre la «mejora de la documentación de identidad de la gente de mar», con vistas a la adopción de un protocolo al Convenio núm. 108 o de otro instrumento y, 15 meses después, la Conferencia adoptó el Convenio núm. 185. Véase OIT: *Actas Provisionales* núm. 27, Conferencia Internacional del Trabajo, 91.ª reunión, Ginebra, 2003, pág. 27/9.

[4] El artículo 9 del Convenio núm. 185 especifica que «Todo Miembro que sea parte en el Convenio sobre los documentos de identidad de la gente de mar, 1958, y esté tomando disposiciones, de conformidad con el artículo 19 de la Constitución de la Organización Internacional del Trabajo, con miras a la ratificación del presente Convenio, podrá notificar al Director General su intención de aplicar el presente Convenio con carácter provisional. Todo documento de identidad de la gente de mar expedido por un Miembro que se halle en esa situación será considerado, a efectos del presente Convenio, como un documento de identidad de la gente de mar expedido en virtud del mismo, siempre que se cumplan los requisitos exigidos en los artículos 2 a 5 del presente Convenio, y que el Miembro interesado acepte documentos de identidad de la gente de mar expedidos de conformidad con dicho Convenio».

B. Breve resumen del Convenio núm. 185 y medidas para apoyar su aplicación

7. El principal objetivo del Convenio núm. 185 es facilitar la admisión temporal de los marinos en un territorio extranjero para que puedan acceder a las instalaciones para el bienestar de la gente de mar que se encuentran en tierra o disfrutar del permiso para bajar a tierra, todo ello a fin de cuidar el bienestar de la gente de mar mientras se encuentra en los puertos y para el tránsito a través de los países en relación con la operación de los buques (para que un marino pueda embarcar en un buque o desembarcar de un buque, por ejemplo para ser repatriado). Estos objetivos y necesidades de la industria, al igual que los servicios que deben proporcionarse a la gente de mar a este respecto, se mantienen inalterados en lo que respecta al Convenio núm. 108. Las importantes innovaciones del Convenio núm. 185 están relacionadas con la introducción de características de seguridad modernas en los materiales utilizados para la confección del nuevo documento de identidad de la gente de mar (DIM) y con las particularidades biométricas de este documento (huella dactilar impresa y fotografía) así como con las particularidades para facilitar la verificación de los DIM (uniformidad y legibilidad por medios mecánicos). También tienen relación con los requisitos mínimos relativos a los procesos y procedimientos de expedición, que incluyen el control de calidad, las bases de datos nacionales y la disponibilidad permanente de los centros nacionales de coordinación que proporcionan información a las autoridades fronterizas. Una característica importante en materia de seguridad es que los DIM ahora sólo pueden ser expedidos y verificados por el país del que son nacionales los marinos [5] y, aunque estos documentos no son considerados documentos de viaje de por sí (por ejemplo, pasaportes o visados), su expedición puede estar sujeta a las mismas condiciones establecidas por las legislaciones nacionales para los documentos de viaje. Por último, tienen relación con un sistema de control internacional a fin de garantizar que los países que han ratificado el Convenio cumplen con esas exigencias mínimas.

8. Cuando, en 2003, se adoptó el Convenio, los participantes en la Conferencia Internacional del Trabajo (CIT) comprendieron que para que pudiera aplicarse plenamente sería necesario desarrollar sus aspectos más técnicos. En una resolución que se adoptó al mismo tiempo que el Convenio núm. 185, la CIT señaló que el éxito del Convenio «dependerá de que cada Miembro que lo ratifique disponga de la tecnología, los conocimientos especializados y los recursos materiales necesarios para la producción y la verificación del nuevo documento de identidad seguro destinado a la gente de mar, previsto en el Convenio, así como para la base de datos y los procesos de expedición correspondientes» [6]. En la resolución se hace referencia a la utilización del programa de cooperación técnica de la Organización, y, en particular, se insta a los Miembros de la OIT a que «convengan en las medidas de cooperación que: *a)* les permitan compartir, cuando proceda, su tecnología, sus conocimientos especializados y sus recursos; *b)* doten a los países de tecnología y procedimientos avanzados a fin de ayudar a los Miembros que estén menos adelantados en estos ámbitos». La Oficina ha llevado a cabo muchas misiones de asistencia técnica a fin de ayudar a los países interesados a ratificar y/o aplicar el Convenio núm. 185, pero no dispone de suficientes recursos presupuestarios para ayudar a muchos países con economías emergentes, de los que proceden muchos de los marinos de todo el mundo, a costear los gastos que implica la utilización de los complejos y seguros sistemas necesarios para expedir los DIM con arreglo a las exigencias del Convenio núm. 185.

[5] El Convenio también prevé que el documento se podrá expedir a los residentes permanentes (artículo 2, 3)).

[6] Resolución relativa a la cooperación técnica en materia de documentos de identidad de la gente de mar, adoptada el 18 de junio de 2003, *Resoluciones adoptadas por la Conferencia Internacional del trabajo en su 91.ª reunión (2003)*, OIT, Ginebra, 2003.

9. En otra resolución adoptada en 2003, la CIT pidió al Consejo de Administración que tomara las disposiciones necesarias para que se elaborase una norma técnica referente a la plantilla biométrica que debía incorporarse al DIM en virtud del párrafo 8 del artículo 3 del Convenio. Esta norma técnica (ILO SID-0002) fue adoptada por el Consejo de Administración en su 289.ª reunión (marzo de 2004) y fue enmendada en su 294.ª reunión (noviembre de 2005) [7].

10. De 2004 a 2008, la Oficina encargó la realización de pruebas con los productos biométricos elaborados conforme a esa norma técnica de la OIT. Doce productos biométricos procedentes de 11 fuentes diferentes cumplen con las exigencias establecidas en dicha norma técnica [8]. Como resultado de los cambios tecnológicos y del desarrollo de normas de control de la seguridad fronteriza, que se han producido desde que en 2008 se realizó la última prueba, la mayor parte de los productos de la lista ya no están disponibles y algunas de las empresas enumeradas ya no son entidades independientes.

11. Las pruebas que se mencionan en el párrafo anterior se presentaron a un órgano técnico mixto de la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (IEC) y el Subcomité sobre Biometría (SC 37) del Comité ISO-IEC JTC 1, que ha estado cooperando con la OIT sobre los aspectos técnicos del Convenio, y en particular en lo que respecta a la elaboración de una norma técnica sobre la plantilla biométrica, y fueron revisadas por estos organismos. El SC 37 también respaldó el Convenio núm. 185 al publicar, en agosto de 2009, tras casi cinco años de trabajo, la norma *ISO/IEC 24713-3:2009 «Tecnología de la información — Perfiles biométricos para la interoperabilidad y el intercambio de datos — Parte 3: Verificación e identificación de la gente de mar basadas en datos biométricos»* [9]. El objetivo de esta norma de la ISO es poner los aspectos técnicos del DIM, tal como se detallan en la norma ILO SID-0002, de conformidad con las normas biométricas mundiales elaboradas por el SC 37 después de la adopción del Convenio núm. 185. También contiene algunas opciones técnicas adicionales para que el DIM sea más seguro, y para que potencialmente sea más eficaz en función de los costos y más fácil de utilizar en los controles fronterizos de todo el mundo.

12. Para examinar cuál es la mejor respuesta al contenido de la norma ISO/IEC 24713-3:2009, y también para entender por qué el ritmo general de ratificación del Convenio núm. 185 ha sido comparativamente lento, el Consejo de Administración decidió celebrar consultas tripartitas con los gobiernos de los Estados Miembros que habían ratificado el Convenio núm. 185 o estaban considerando seriamente la posibilidad de ratificarlo, y las organizaciones internacionales de armadores y de gente de mar. Esas consultas se celebraron en septiembre de 2010 [10].

[7] La versión actual de la norma ILO SID-0002 se puede consultar en: http://www.ilo.org/wcmsp5/groups/public/@ed_norm/@normes/documents/genericdocument/wcms_144265.pdf.

[8] En la página Web que figura a continuación se publica una lista de esos productos y de sus distribuidores: http://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/publication/wcms_191713.pdf.

[9] En la siguiente página Web de la ISO se pueden adquirir copias de esta norma: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50683.

[10] El informe de las consultas se presenta en el documento CSID/C.185/2010/4, disponible en: http://www.ilo.org/wcmsp5/groups/public/@ed_norm/@normes/documents/meetingdocument/wcms_150402.pdf.

13. El consenso alcanzado en esas consultas [11] incluye sugerencias en aras de la aceptación de cambios técnicos menores en el contenido del DIM, tal como se recomienda en la norma ISO/IEC 24713-3:2009, y también de algunos cambios más importantes a fin de que el sistema internacional de DIM expedidos y verificados por diferentes países sea más seguro y fácil de utilizar. Las sugerencias incluyen:

a) actualizar determinados detalles del código de barras bidimensional incorporado al DIM;

b) modificar el código de barras de suerte que en él se integre una firma digital;

c) establecer un centro internacional encargado de coordinar los centros nacionales de coordinación u ofrecer un acceso seguro a las bases electrónicas de datos mencionadas en el artículo 4 del Convenio núm. 185;

d) en relación con los datos referentes a las huellas dactilares, convenir en que, aunque las bases de datos nacionales sólo pueden contener la plantilla biométrica prevista en el Convenio, también sea posible almacenar en ellas, a instancia de los marinos interesados, una imagen de las huellas dactilares para simplificar su reinscripción;

e) prever la opción de incorporar, además, un microchip al DIM que pueda ser compatible con el lector estándar de pasaportes electrónicos; y

f) organizar una licitación internacional que desemboque en la confección de una lista de vendedores cualificados y capaces de surtir los componentes de un sistema de expedición de DIM a precios razonables, licitación que la Oficina podría llevar a cabo o propiciar.

14. La Oficina intentó encontrar mecanismos para poner en práctica esas sugerencias, y finalmente las señaló de nuevo a la atención del Consejo de Administración, tal como se indica en el párrafo 1. Esas sugerencias, junto con algunas otras cuestiones, se exponen más detalladamente en el capítulo III de este documento.

15. Durante ese período, la Oficina se encargó de preparar la infraestructura necesaria para examinar la documentación y la información que los Miembros signatarios faciliten para su inclusión en la lista de los Miembros que cumplen cabalmente los requisitos mínimos estipulados en el Convenio en relación con los procesos y procedimientos de expedición de DIM, entre ellos los procedimientos de control de calidad. El párrafo 6 del artículo 5 del Convenio establece que el Consejo de Administración debe aprobar esa lista con arreglo a las disposiciones que él mismo haya adoptado. En esas disposiciones, que se adoptaron en 2005 [12], se indican la documentación y la información exigidas y se confía a un Grupo de examen y a un Comité especial de examen la responsabilidad de prestar asesoramiento al Consejo de Administración en relación con esa lista. El Grupo de examen y el Comité especial de examen fueron instituidos por el Consejo de Administración en 2010 y 2011 [13]

[11] *Ibíd.,* anexo I, Resumen del consenso alcanzado en las Consultas de la OIT relativas al Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185).

[12] Documento GB.292/LILS/11, anexo I, Disposiciones referentes a la lista de los Miembros que cumplen cabalmente los requisitos mínimos relativos a los procesos y procedimientos de expedición de los documentos de identidad de la gente de mar, disponible en: http://www.ilo.org/public/english/standards/relm/gb/docs/gb292/pdf/lils-11.pdf.

[13] Documento GB.309/18/6.

No obstante, la presentación de la información que debe ser estudiada, incluidos los informes de las evaluaciones independientes, ha sido lenta.

16. Desde que en 2002 se realizaron los primeros debates acerca de la revisión del Convenio núm. 108, la Organización Marítima Internacional (OMI) ha sido una aliada fundamental de la OIT a fin de garantizar que los marinos puedan acceder a los servicios que necesiten en tierra, y que se otorguen permisos para bajar a tierra a los marinos que tengan derecho a ellos como un elemento de la aplicación de un convenio de la OMI [14]. En 2004, tanto la OIT como la OMI aprobaron el *Repertorio de recomendaciones prácticas sobre protección en los puertos de la OMI/OIT* [15], que fue elaborado conjuntamente por un grupo de trabajo de ambas organizaciones. En ese documento se recomienda que todos los planes de protección portuaria incluyan procedimientos para facilitar el movimiento de la gente de mar, incluidos los representantes de las organizaciones para el bienestar de la gente de mar y las organizaciones de trabajadores, y su acceso a los puertos, las instalaciones de los puertos y los buques, según proceda. También se indica que los DIM expedidos en virtud del Convenio núm. 185 de la OIT han de satisfacer todos los requisitos de ese Repertorio de recomendaciones prácticas a efectos de identificación y acceso. El 27 de mayo de 2010, la OMI emitió la Circular 1342 del Comité de Seguridad Marítima, en la que se recuerdan a los Estados sus obligaciones en virtud del Convenio internacional sobre la seguridad de la vida humana en el mar, de 1974 (SOLAS) y el Código internacional para la protección de los buques y de las instalaciones portuarias (Código PBIP) de velar por que todos los planes de protección portuaria contemplen la necesidad de la gente de mar de bajar a tierra y el acceso a las instalaciones de bienestar y a la asistencia médica en tierra. El 4 de diciembre de 2013, la Asamblea de la OMI adoptó la resolución, «Trato justo de los tripulantes por lo que respecta al permiso de tierra y al acceso a las instalaciones en

[14] El Convenio de la OMI para facilitar el tráfico marítimo internacional (FAL), en su forma enmendada, fue adoptado en 1965. En este Convenio se reconoce, entre otras cosas, que para las operaciones marítimas es muy importante que la gente de mar pueda transitar fácilmente por los países a fin de embarcar en buques o desembarcar de ellos. En la Norma 3.10 se estipula que «Un pasaporte o un documento de identidad expedido de conformidad con los convenios pertinentes de la OIT o, si no, un documento de identidad para gente de mar válido y debidamente reconocido, será el documento básico que facilite a las autoridades públicas los datos sobre cada uno de los tripulantes, a la llegada o salida de los buques». También se prevé que no se exigirá visado a la gente de mar para disfrutar del permiso para bajar a tierra. En la Norma 3.44 se establece que «Las autoridades públicas permitirán que los tripulantes extranjeros desembarquen mientras permanezca en puerto el buque en que hayan llegado, siempre que se hayan cumplido los trámites pertinentes a la llegada del buque y las autoridades públicas no tengan motivos para negarse a conceder permiso de desembarco por razones de higiene, seguridad u orden públicos». En la Norma 3.45 se prevé que «No se exigirá visado a los tripulantes para que puedan gozar del permiso de tierra». En su último período de sesiones, el Comité de Facilitación de la OMI aprobó, con el objeto de modernizar el Convenio, un anexo revisado que incluye normas sobre el permiso para bajar a tierra y el acceso de los tripulantes a las instalaciones de tierra, y se agregó la siguiente disposición a la Norma 3.44: «El permiso de tierra se autorizará de manera tal que excluya cualquier discriminación por razón de nacionalidad, raza, color, sexo, religión, opinión política u origen social, e independientemente del Estado de abanderamiento del buque en el que estén empleados, contratados o trabajen». Asimismo se propuso una nueva Norma 3.44*bis*: «En todos los casos en que se haya denegado el permiso en tierra, las autoridades públicas comunicarán los motivos alegados para dicha denegación al marino interesado y al capitán. Si éstos lo solicitan, tales motivos se proporcionarán por escrito». Véase OMI: FAL 39/16 (2 Oct. 2014), Comité de Facilitación, 39ª período de sesiones, 22-26 de septiembre de 2014. Este documento se distribuirá con miras a su adopción en el próximo período de sesiones del Comité que se celebrará en marzo-abril de 2016.

[15] Este repertorio fue debatido en la Reunión tripartita de expertos sobre vigilancia, seguridad y salud en los puertos (Ginebra, 2003) y está disponible en línea en: http://www.oas.org/cip/docs%5Cdocumentos_importantes%5CILOIMOCODEDRAFTmesshp-cp-aSpanish.pdf.

tierra» [16] , en la que se reconoce que «los tripulantes son una categoría especial de trabajadores que, por el carácter mundial del sector del transporte marítimo y las diferentes jurisdicciones, especialmente las distintas autoridades públicas con las que puede entablar contacto, requiere una protección especial».

17. Asimismo, la Oficina ha trabajado con la Organización de Aviación Civil Internacional (OACI), dado que el Convenio núm. 185 especifica en el anexo I que «El material utilizado en la producción del documento, sus dimensiones y la disposición de los datos se ajustarán a las normas de la Organización de Aviación Civil Internacional (OACI) aplicables a los pasaportes de lectura mecánica, con arreglo a lo indicado en la Parte 3 del documento núm. 9303 (2.ª edición, 2002), o la Parte 1 del documento núm. 9303 (5.ª edición, 2003)». Si bien la secretaría de la OACI respaldó firmemente esta idea e inicialmente indicó que ayudaría a los gobiernos a aplicar el Convenio núm. 185 verificando que los DIM satisficieran plenamente los requisitos que figuran en el documento núm. 9303 de la OACI, posteriormente no hubo recursos para proporcionar esta ayuda. Lamentablemente, cuando en 2006 y 2008 se publicaron nuevas ediciones de la parte 1 y la parte 3 del documento núm. 9303, las versiones que se especifican en el anexo I del Convenio núm. 185 se retiraron y ya no se encuentran disponibles para los gobiernos que quieren aplicar el Convenio núm. 185.

18. La Oficina se puso en contacto con la secretaría de la OACI para tratar de resolver estas cuestiones, pero no consiguió el apoyo del Grupo de trabajo sobre nuevas tecnologías del Grupo técnico asesor sobre los documentos de viaje de lectura mecánica de la OACI, que controla el contenido del documento núm. 9303 de la OACI.

19. Si bien el Convenio núm. 185 no se incluyó en el MLC, 2006, tal como se mencionó en el párrafo 5, en el MLC, 2006, se subraya la importancia del permiso para bajar a tierra para la salud y el bienestar de la gente de mar. El MLC, 2006, no trata la cuestión de los documentos de identidad, pero en el párrafo 1 de la Regla 4.4 se estipula que «Los Miembros deberán velar por que las instalaciones de bienestar en tierra, si las hay, sean de fácil acceso» y en el párrafo 5 de la Pauta B4.4.6 se recomienda que «Los responsables en los puertos y a bordo deberían esforzarse al máximo por que se autorice a la gente de mar a desembarcar tan pronto como sea posible tras la llegada del buque a puerto».

III. Opciones a examinar en relación con la aplicación del Convenio núm. 185

20. Tal como se señaló en la sección anterior de este documento, las necesidades de la gente de mar y de la industria naviera condujeron a la adopción del Convenio núm. 108 de 1958. No obstante, tras los eventos del 11 de septiembre de 2001, se adoptó el Convenio núm. 185 con miras al establecimiento de un sistema de identificación de la gente de mar eficaz en relación con el costo y seguro. Este sistema se basa en las tecnologías que existían en 2003, que han sido superadas por nuevas tecnologías e infraestructuras que han conducido, por ejemplo, al desarrollo de los nuevos pasaportes electrónicos y también, en algunas regiones, a la expedición de documentos biométricos independientes para «viajeros de confianza» que permiten pasar más rápidamente los controles fronterizos a ciertas categorías de viajeros, con frecuencia personas que regularmente realizan viajes internacionales y han solicitado el documento y superado las pruebas para obtenerlo.

[16] Resolución A. 1090 (28).

21. No obstante, en el Convenio núm. 185 se tuvo en cuenta, de manera única cuando se adoptó el Convenio e incluso actualmente, la necesidad de ofrecer a la gente de mar mejores servicios que los que se ofrecen a los otros trabajadores, debido a sus condiciones especiales de trabajo y a la necesidad de facilitar el funcionamiento de las actividades marítimas — en particular, a la necesidad de que la gente de mar pueda entrar en un territorio extranjero en un breve plazo para disfrutar de su licencia en tierra firme o para embarcar en buques o desembarcar de ellos. Esa característica única del Convenio núm. 185 tiene relación con el aumento de la fiabilidad del documento de identidad de la gente de mar (DIM), y con el hecho de que el DIM sólo podrá ser expedido: *a)* por la autoridad que está en la mejor posición para controlar la buena fe de las personas que dicen ser marinos, a saber el Estado del que las personas interesadas son nacionales o en el que tienen residencia permanente, y *b)* de conformidad con las normas mínimas. Estas normas incluyen el mantenimiento de una base de datos nacional que contenga el registro de cada DIM que se haya expedido y la designación de un centro permanente de coordinación que pueda proporcionar una respuesta inmediata a las solicitudes de información cursadas por los servicios de inmigración u otras autoridades competentes en relación con la autenticidad y la validez de determinados DIM. Asimismo, incluyen medidas para velar por el respeto del derecho a la privacidad y otros derechos de la gente de mar que solicita DIM. El Miembro de la OIT que ratifique el Convenio también debe hacerse responsable de la fiabilidad de su sistema de DIM, y tendrá que tomar medidas para que se efectúen evaluaciones independientes que someterá al control de la comunidad internacional.

22. Por consiguiente, todas las medidas a fin de mejorar la relación coste-eficacia de los sistemas de DIM tendrán que tener en cuenta la responsabilidad y rendición de cuentas de cada Miembro que haya ratificado el Convenio en relación con los DIM que haya expedido a sus nacionales o residentes permanentes y la necesidad de continuar velando por que en ese proceso se respeten los derechos de la gente de mar.

23. Las opciones que se examinan en este documento para mejorar la aceptación y la utilización de los DIM expedidos en virtud del Convenio núm. 185 pueden dividirse en dos categorías básicas:

a) **Opciones para los Miembros que han ratificado el Convenio núm. 185 o tienen previsto hacerlo.** Habida cuenta de los cambios que se han producido en las tecnologías y en las infraestructuras de control fronterizo, puede resultar necesario cambiar la forma o el contenido de los DIM o la manera de expedirlos, con lo cual el sistema de DIM será más seguro, cómodo y eficaz en función de su costo y, en última instancia, gozará de más reconocimiento para agilizar la entrada de los marinos con arreglo a los actuales requisitos en materia de control fronterizo. **La viabilidad y posibles costos de estas opciones se examinan en la sección A que figura a continuación.**

b) **Opciones para los Miembros que no han ratificado el Convenio núm. 185** en relación con cambios en la forma en que toman decisiones acerca de permitir que los marinos entren en su territorio cuando la entrada tenga por fin el disfrute de un permiso para bajar a tierra, el tránsito, el reembarco en otro buque, o la repatriación. En estas opciones se tiene en cuenta, de conformidad con las legislaciones y las prácticas nacionales, la seguridad adicional que aporta la utilización de DIM expedidos con arreglo al Convenio núm. 185. Son más pertinentes para los Miembros que aún no han ratificado el Convenio núm. 185 pero quieren reconocer las ventajas que éste ofrece en materia, por una parte, de respeto al bienestar de la gente de mar y facilitación del transporte marítimo y, por otra parte, de seguridad adicional. **La viabilidad y posibles costos de estas opciones se examinan en la sección B que figura a continuación.**

24. Cabe señalar que algunas de las opciones que se examinan en la sección A, como por ejemplo la incorporación de un chip electrónico que pueda ser leído por un lector de pasaportes electrónicos, tendrían un impacto tanto en los países que han ratificado el Convenio núm. 185 como en los países que, aunque no lo hayan ratificado, deseen beneficiarse de la seguridad adicional que éste ofrece.

A. Opciones para los Miembros que han ratificado el Convenio núm. 185 o tienen previsto hacerlo en relación con el contenido y la expedición de los DIM

25. Como se explicó previamente, una de las dificultades que se plantean tiene relación con que si bien los sistemas y documentos previstos con arreglo al Convenio núm. 185 tienen importantes ventajas que los hacen únicos en comparación con todos los otros sistemas y documentos internacionales de identidad, las tecnologías e infraestructuras de control fronterizo han cambiado mucho desde 2003 y se han desarrollado otros enfoques. La cuestión que se plantean los Estados Miembros, especialmente los que de buena fe han realizado importantes inversiones para aplicar el Convenio núm. 185, es si tienen que continuar desarrollando las infraestructuras tal como se prevén en las disposiciones del Convenio o si resulta necesario introducir cambios y, en caso de que se requieran cambios, cuáles deben ser. Como se señala a continuación, el hecho de que cada vez haya menos equipos y proveedores autorizados con arreglo al Convenio núm. 185 también es un factor que hay que tener en cuenta.

26. En las secciones A-1 a A-7 se exponen las opciones en relación con el contenido de los DIM (A-1 a A-5) y con el marco institucional (A-6 y A-7). Además, en esas secciones se formulan consideraciones en relación con la viabilidad y el coste de cada opción. Las diversas opciones, excepto la opción A-5, pueden utilizarse al mismo tiempo. Se trata de las siguientes opciones:

A-1. Actualizaciones menores del contenido de los DIM a fin de reflejar las normas más recientes

A-2. Respaldar la continua compatibilidad de las huellas dactilares

A-3. Incorporación de una firma digital al código de barras de los DIM

A-4. Elaboración de DIM que funcionen con chips

A-5. Cambiar los datos biométricos, a saber cambiar la huella dactilar almacenada en un código de barras por una imagen facial

A-6. Establecimiento de una entidad de coordinación de centros de coordinación

A-7. Colaboración entre los Miembros para establecer sistemas de expedición de DIM

A-1. Actualizaciones menores del contenido de los DIM a fin de reflejar las normas más recientes

27. Una cuestión relacionada con los cambios tecnológicos que se han producido desde 2003, que ya se ha mencionado, es que todas las normas externas en relación con los requisitos técnicos que se mencionan en el Convenio núm. 185 y en los documentos técnicos conexos, como la norma ILO SID-0002, que se utilizaban en 2003 y 2004 fueron elaboradas por otras organizaciones (la OACI y la ISO). Los documentos en los que figuran esas normas técnicas fueron revisados durante la última década y ya no se pueden

utilizar. Por ejemplo, en el anexo I del Convenio núm. 185 se estipula que «El material utilizado en la producción del documento, sus dimensiones y la disposición de los datos se ajustarán a las normas de la Organización de Aviación Civil Internacional (OACI) aplicables a los pasaportes de lectura mecánica, con arreglo a lo indicado en la Parte 3 del documento núm. 9303 (2.ª edición, 2002), o la Parte 1 del documento núm. 9303 (5.ª edición, 2003)». Habida cuenta de que esas versiones del documento núm. 9303 ya no pueden obtenerse en la OACI, es difícil que los Estados Miembros que han puesto en marcha un sistema de DIM puedan saber si cumplen adecuadamente con las exigencias técnicas del Convenio. Asimismo, la plantilla biométrica de las huellas dactilares almacenada en un código de barras bidimensional, que se prevé en la norma ILO SID-0002, se basa en un proyecto de norma ISO/IEC 19794-2:2005. La versión final de la norma difería ligeramente del proyecto y desde 2005 ha sido objeto de numerosas modificaciones y correcciones y en 2011 fue sustituida por una versión totalmente nueva, a saber la norma ISO/IEC 19794-2:2011. Las otras normas de la ISO que se mencionan en la norma ILO SID-0002, tales como el proyecto de norma ISO/IEC 19784 utilizada en la interfaz de programación de soluciones biométricas (BioAPI) en relación con la codificación de huellas digitales, también se han actualizado ampliamente durante los últimos años. Las actuales normas técnicas en relación con los DIM previstos en el Convenio núm. 185 son obsoletas debido a que ya no están de conformidad con las normas internacionales que se están utilizando en otros sistemas biométricos y de documentos de identidad.

28. La forma más sencilla de resolver este problema sería actualizando tanto el anexo I del Convenio núm. 185 como la norma ILO SID-0002 a fin de reflejar las últimas normas internacionales. Esto implicaría revisar esos documentos en profundidad para incluir en ellos todos los elementos técnicos de las normas de la OACI y la ISO con miras a que ya no fuera necesario remitir a los documentos de la OACI o la ISO. Sin embargo, la OIT no es una fuente mundial de conocimientos en materia de biometría y documentos de identidad, y los grupos pertinentes de la OACI y la ISO pueden dedicar mucho más tiempo y más recursos a estas cuestiones. Sería sumamente difícil reproducir todos los esfuerzos realizados por la OACI y la ISO en esta materia y, aunque en un momento dado esto pudiera hacerse, se correría el riesgo de que en el futuro existieran por una parte las normas internacionales reconocidas y las normas técnicas de la OIT que figurarían en el anexo I revisado del Convenio núm. 185 y en la norma ILO SID 0002.

29. Una solución más duradera podría ser retirar totalmente la norma ILO SID-0002 y revisar los anexos I y II del Convenio núm. 185 a fin de que no incluyan detalles técnicos y sólo proporcionen directrices generales en las que se haga referencia a versiones sin fecha de los documentos pertinentes de la OACI y la ISO. Entonces cuando cada Miembro de la OIT estableciera un sistema de DIM tendría que asegurarse de que seguía las últimas versiones de las normas pertinentes de la OACI y la ISO. Con esto se garantizaría que los DIM siempre fueran compatibles con los pasaportes y las tarjetas encartadas en los pasaportes, tal como las define la OACI, y que siempre se beneficiaran de la última tecnología tal como se define en las normas de la ISO en materia de biometría. Siempre se pueden plantear problemas de compatibilidad «hacia atrás», pero, como también se trata de una cuestión muy importante para los que expiden pasaportes, la OACI deja que transcurran períodos de tiempo muy largos antes de retirar las tecnologías antiguas. Asimismo, la OACI mantiene el contacto con la ISO a fin de garantizar que las normas biométricas de la ISO que se utilizan para los pasaportes electrónicos están disponibles durante todo el tiempo en que sean necesarias para los que expiden pasaportes siguiendo las directrices de la OACI. Actualmente, la OIT mantiene un contacto de categoría A con el SC 37, que es el grupo responsable de todas las normas biométricas, y puede utilizar este contacto a fin de garantizar que las normas antiguas que están siendo utilizadas por los que expiden DIM no se retiren con excesiva rapidez.

30. Cabe señalar que con la elaboración de la norma ISO/IEC 24713-3:2009 *Tecnología de la información — Perfiles biométricos para la interoperabilidad y el intercambio de datos —*

Parte 3: Verificación e identificación de la gente de mar basadas en datos biométricos ya se ha realizado la mayor parte del trabajo para determinar exactamente cómo utilizar las actuales normas biométricas de la ISO en apoyo de los DIM. Si bien este documento está protegido por los derechos de autor de que es titular la ISO y no puede reproducirse completamente, algunos de los artículos pertinentes para la revisión del código de barras bidimensional a fin de adaptarlo a las actuales normas de la ISO e incorporar una firma digital (que se examinará en la sección A-3) figuran en el anexo II del presente documento a fin de ilustrar el trabajo que ya se ha realizado. Por ejemplo, en uno de los artículos que se han incluido en el extracto ilustrativo de la norma de la ISO figuran los elementos que debe contener la base electrónica de datos nacional e información más detallada que la que figura en el anexo II del Convenio núm. 185. Asimismo, se indica que en la base de datos se podrían incluir imágenes de las huellas dactilares que correspondan a las plantillas almacenadas en los DIM. Esto se considera una buena práctica debido a que si la tecnología que se utiliza para codificar las huellas dactilares cambiara durante el período de validez del DIM de un marino permitiría reinscribir automáticamente a ese marino y expedirle un nuevo DIM sin que tuviera que acudir a una oficina.

Opción A-1. Proyecto de recomendación que se somete a discusión

31. El Consejo de Administración de la OIT podría solicitar a la Oficina que prepare un proyecto preliminar de texto revisado de los anexos I y II del Convenio núm. 185 en el que los detalles técnicos del código de barras bidimensional y la base electrónica de datos nacional se basen en la norma ISO/IEC 24713-3, y el formato y la presentación del DIM se basen en el documento núm. 9303 de la OACI, y que contemple futuras modificaciones de esos documentos a fin de que puedan realizarse cambios tecnológicos sin que sea necesario revisar los anexos.

32. Las versiones provisionales se someterían a un órgano marítimo tripartito de la OIT debidamente constituido con miras a que la CIT modificara esos anexos de conformidad con el artículo 8 del Convenio núm. 185.

33. Asimismo, el Consejo de Administración podría pedir a la Oficina que mantenga el contacto con el SC 37 a fin de garantizar que la norma ISO/IEC 24713-3 sigue disponible y se actualiza periódicamente a fin de reflejar los cambios tecnológicos.

- **Principales beneficios de la recomendación**

  Con arreglo al Convenio núm. 185, los DIM se mantendrían al día en lo que respecta a los cambios en el diseño y la presentación de los pasaportes, y a las tecnologías biométricas, y seguirían cumpliendo las principales normas internacionales sin que la OIT tuviera que adoptar ninguna otra medida excepto mantener el contacto con el SC 37.

- **Costo de la recomendación y problemas que pueden plantearse**

  Introducir las modificaciones necesarias en el software de los sistemas existentes de DIM a fin de ajustarlo a las nuevas versiones de las normas en la materia costaría probablemente entre 10 000 y 50 000 dólares de los Estados Unidos a cada país que ya haya establecido un sistema de DIM. La Oficina tendría gastos regulares para mantener el contacto con el SC 37, ya que esto requeriría enviar a un delegado al menos a una reunión al año. Los cambios futuros en las normas técnicas probablemente requerirían una actualización, aproximadamente cada cinco o diez años, de los sistemas existentes de DIM, lo cual serviría para que esos sistemas siguieran estando en consonancia con las normas internacionales.

A-2. Respaldar la continua compatibilidad de las huellas dactilares

34. La representación biométrica que se menciona en el párrafo 8 del artículo 3 del Convenio núm. 185 actualmente se define como una plantilla de la huella dactilar creada a partir de minucias basada en una versión provisional de la norma ISO/IEC 19794-2:2005. Habida cuenta de que se trata de una plantilla y no de una imagen, sólo puede ser utilizada en sistemas de huellas dactilares que se adecuan a esta forma particular de plantilla normalizada a partir de minucias. Lamentablemente, no existe un programa mundial de certificación para los sistemas de huellas dactilares que utilicen una plantilla a partir de minucias basada en la norma ISO/IEC 19794-2:2005. Por consiguiente, la OIT tuvo que realizar pruebas con los productos de huellas dactilares a fin de garantizar la posibilidad de: registrar las huellas dactilares de los marinos; crear una plantilla con esas huellas en un formato adecuado; leer la plantilla, y verificar las huellas dactilares generadas por todos los otros sistemas compatibles. Esas pruebas se realizaron en 2004, 2006 y 2008 y llevaron a crear la lista de productos de la OIT [17]. Sin embargo, desde 2008 no se ha llevado a cabo ninguna prueba. Esto se debe principalmente a que las pruebas pertinentes son costosas y a que la OIT no ha contado con los fondos de cooperación técnica necesarios para financiar otra ronda de pruebas. Los gobiernos tampoco han invertido lo suficiente en sistemas conformes con la norma ILO SID a fin de incentivar a las empresas que fabrican productos de huellas dactilares para que costeen las pruebas de sus productos y de esta forma puedan ser incluidas en la lista de la OIT.

35. En la lista actual figuran 12 productos, cada uno de los cuales consiste en un algoritmo de huellas dactilares combinado con un sensor de huellas dactilares. Entre 2004 y 2008 esos productos contenían tecnología actualizada en materia de huellas dactilares pero han quedado desfasados. Otro problema es que muchas de las empresas que suministraban sistemas de huellas dactilares se fusionaron con otras empresas y puede que algunas de ellas ya no suministren esos productos. Además, el mercado de sistemas de DIM es muy reducido en comparación con el mercado de sistemas para los otros documentos de identidad y algunas de las empresas ya no están interesadas en el mercado de DIM. Por último, muchos de los componentes de los sensores de los productos que figuran en la lista de productos aprobados ya no se fabrican y todos los algoritmos de los productos han sido reemplazados por algoritmos más nuevos y precisos. En 2014, los gobiernos de dos Estados Miembros que han ratificado el Convenio núm. 185 informaron a la OIT de las grandes dificultades que han tenido últimamente para encontrar nuevos proveedores de productos biométricos aprobados y también indicaron que han tenido problemas para conseguir asistencia técnica para los sistemas de DIM existentes. Esto está probablemente relacionado con el reducido número de DIM que se expiden y con el hecho de que pocos países utilicen estos sistemas, lo cual lleva a que la expedición de DIM no sea un buen negocio para la mayor parte de empresas que venden sistemas de expedición de documentos y productos biométricos.

36. Si no se dispone de una lista de productos que han sido objeto de pruebas o de algún otro medio que sirva para garantizar que los sistemas biométricos son objeto de pruebas apropiadas es imposible saber si un DIM expedido en el país A que utiliza el producto biométrico X podrá ser utilizado para verificar las huellas dactilares de los marinos en la frontera cuando éstos quieran entrar en el país B que utiliza el producto biométrico Y. Las normas internacionales son un requisito previo para la interoperabilidad, pero no la garantizan.

[17] Esta lista de 12 productos se puede consultar en: http://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/publication/wcms_191713.pdf.

37. Una posible solución a este problema sería seleccionar un solo producto biométrico y exigir que se utilice en todos los sistemas de expedición y de verificación de DIM. Esto, sin embargo, implicaría otorgar el monopolio a un solo vendedor y representaría un riesgo potencial de que el vendedor aumentara los precios o abandonara el negocio.

38. Otra posible solución consistiría en cambiar la plantilla con datos biométricos prevista para el DIM por otro tipo de plantilla de huellas dactilares que ya se esté utilizando en otro sitio y cuya interoperabilidad sea objeto de pruebas regulares. El único ejemplo conocido de plantilla de huellas dactilares distribuida por diferentes proveedores de productos biométricos cuya interoperabilidad es objeto de pruebas regulares es la plantilla 378 de la Comisión Internacional para las Normas relativas a las Tecnologías de la Información especificada por el Gobierno de los Estados Unidos para el programa de verificación de la identidad personal (PIV), cuya interoperabilidad ha sido objeto de pruebas en el Instituto Nacional de Normalización y Tecnología de los Estados Unidos en el marco del programa Minutia Exchange (MINEX). Utilizar esta plantilla haría que toda la responsabilidad en relación con probar los productos de huellas dactilares recayera en un gobierno y conduciría a utilizar una norma nacional en lugar de una norma internacional, aunque podría tratarse de un cambio aceptable si condujera a un sistema de DIM interoperable que se mantuviera al día en lo que respecta a la tecnología actual. Dado que en el marco del programa MINEX sólo se efectúan pruebas de algoritmos, las pruebas para medir el efecto de los diversos sensores de huellas dactilares sobre la interoperabilidad no se reemplazarían. Esto podría resolverse separando los actuales productos biométricos en algoritmos y sensores, y exigiendo que los algoritmos tengan la certificación del programa MINEX y que los sensores tengan la certificación del programa PIV de la Oficina Federal de Investigaciones de los Estados Unidos.

39. Si se utilizara una norma nacional podrían plantearse diversos problemas. En primer lugar, en cualquier momento el gobierno podría cambiar la norma a fin de cumplir con los requisitos internos y la compatibilidad «hacia atrás» no sería necesariamente una prioridad. En segundo lugar, no existiría garantía alguna de que el gobierno interesado continuara manteniendo la lista de productos certificados por el programa MINEX. Esto conduciría a que la interoperabilidad del sistema mundial de DIM dependiera de la continuación de un determinado programa nacional de documentos de identidad. En tercer lugar, la norma PIV aún no es una norma internacional y, por consiguiente, no ha sido reconocida por la ISO o la OACI. Esto significa que si la OIT decidiera utilizar productos certificados por los programas PIV y MINEX no podría utilizar directamente la norma ISO/IEC 24713-3 y tendría que crear un documento totalmente nuevo para explicar cómo se tiene que utilizar la norma PIV en el contexto de los DIM. Esto requeriría esfuerzos considerables en un ámbito que no es una de las esferas normales de especialización de la OIT y ésta no podría basarse en los conocimientos de la OACI o la ISO. Probablemente se tardaría al menos un año en elaborar un documento de ese tipo y la contratación de expertos externos a fin de elaborarlo y revisarlo costaría entre 50 000 y 100 000 dólares de los Estados Unidos.

40. Si la solución nacional antes mencionada no resulta viable, la única alternativa posible en este momento es que la OIT decida asignar fondos suficientes para costear nuevas rondas de pruebas siguiendo un ciclo tecnológico razonable, por ejemplo cada tres años. Cada ciclo de pruebas costaría aproximadamente 150 000 dólares de los Estados Unidos, lo que representaría un gasto anual de aproximadamente 50 000 dólares de los Estados Unidos.

Opción A-2. Proyecto de recomendación que se somete a discusión

41. El Consejo de Administración de la OIT podría solicitar a la Oficina que busque la financiación de los Miembros interesados a fin de realizar inmediatamente una ronda de pruebas de interoperabilidad con miras a modificar la actual lista de la OIT de productos sometidos a prueba. Todos los productos que figuran en la lista se someterían a nuevas pruebas y todos los nuevos proveedores que ofrecieran productos adecuados de huellas

dactilares serían invitados a participar en esas pruebas. A fin de permanecer en la lista o de entrar en ella, la empresa debería indicar su voluntad de participar en la nueva ronda de pruebas y de continuar poniendo a la venta durante un período de tres años, a partir del momento de la publicación de los resultados de la prueba, el mismo modelo de sensor de huellas dactilares y la misma versión de algoritmo para los procesos de registro y correspondencia de datos. La Oficina repetiría estas pruebas cada tres años.

- **Principales beneficios de la recomendación**

  El sistema mundial de DIM seguiría siendo interoperable y en la lista de productos sólo figurarían productos que se encontraran en el mercado y que seguirían estándolo al menos hasta que se realizara otra ronda de pruebas de interoperabilidad. El sistema de DIM seguiría estando sujeto a las normas internacionales y su continua interoperabilidad estaría controlada por la OIT. La exigencia de que los productos estuvieran disponibles durante un período mínimo de tiempo permitiría suprimir de la lista a las empresas que ya no fabricaran los productos aprobados, y garantizaría que todos los productos que figuraran en la lista estuvieran disponibles al menos durante los tres años posteriores a la publicación de la lista.

- **Costo de la recomendación y problemas que pueden plantearse**

  La OIT tendría que conseguir una financiación sostenible para un presupuesto trianual de aproximadamente 150 000 dólares de los Estados Unidos. Esta financiación podría proceder de los fondos disponibles o de la contribución de uno o más Estados Miembros interesados en establecer un sistema de DIM o que quieran actualizar el sistema que han establecido. Se eliminarían de la lista de productos interoperables los productos de empresas que dejaran de existir o perdieran su interés en el mercado de DIM, lo cual conduciría a que algunos países tuvieran que cambiar la tecnología en materia de huellas dactilares que utilizan en su sistema de DIM. Sin embargo, teniendo en cuenta que en principio los cambios sólo se producirían cada tres años y que es muy probable que las empresas que han vendido productos continúen estando interesadas en este mercado, este problema no debería plantearse con mucha frecuencia. Pero en el caso de que se planteara, las pruebas de interoperabilidad implicarían que sólo tendrían que sustituirse los sensores y algoritmos de huellas dactilares que, en general, sólo representan entre el 5 y el 10 por ciento del costo de un sistema de DIM.

A-3. Incorporación de una firma digital al código de barras de los DIM

42. Durante la elaboración de la norma ISO/IEC 24713-3:2009, los expertos técnicos del SC 37 tomaron nota de que el DIM actual no es tan seguro como muchos otros documentos de identidad, como por ejemplo los pasaportes, debido a que se basa totalmente en la seguridad física y carece de seguridad digital. Además, tampoco tiene un alto nivel de seguridad física [18], lo cual hace que actualmente sea relativamente fácil falsificar un DIM. La falsificación de pasaportes es un problema de larga data e

[18] En el anexo I del Convenio núm. 185 se estipula que «Las páginas previstas para los datos indicados a continuación, en negritas, estarán protegidas por una lámina o revestimiento, o mediante la utilización de una tecnología de imagen y un material de base que garanticen una resistencia equivalente contra toda sustitución de la fotografía y demás datos biográficos» y que «Entre las demás características relativas a la seguridad, deberá incluirse al menos una de las siguientes: filigranas, marcas ultravioleta, tintas y dibujos de colores especiales, imágenes perforadas, hologramas, grabados en láser, microimpresión y plastificación en caliente».

históricamente ha redundado en una lucha continua entre los que expiden documentos y los que los falsifican a medida en que se introducían características de seguridad física más elaboradas. Por ejemplo, el pasaporte electrónico se diseñó para que al utilizar la seguridad de la criptografía digital que tiene una intensidad de algoritmo conocida y, por consiguiente, ofrece un nivel conocido (muy elevado) de seguridad y resistencia a las falsificaciones se eliminara ese problema.

43. El Convenio núm. 185 no contempla la utilización de la criptografía como técnica de seguridad debido a que el pasaporte electrónico no existía cuando se adoptó el Convenio y la utilización de las firmas digitales en los documentos de identidad no se había consolidado. Cuando se elaboró la norma ISO/IEC 24713-3, el SC 37 utilizó la norma ISO/IEC 19785-1:2006 relativa al marco común de formatos de intercambio de datos biométricos (CBEFF) a fin de crear el «envoltorio» para que los datos de la plantilla de huellas dactilares se codificaran en el DIM. Introducir datos biométricos en una estructura del CBEFF es algo bastante común cuando se trata de documentos de identidad con elementos biométricos y es una técnica que se utiliza en los pasaportes electrónicos de la OACI. Una ventaja del CBEFF es que ofrece la opción de incluir un bloque de seguridad que utiliza una firma digital para garantizar que los datos que figuran en su registro no han sido manipulados. Para la norma ISO/IEC 24713-3 se creó una estructura del CBEFF poco habitual y muy compacta que se describe en los artículos del extracto de ese documento que figuran en el **anexo II** del presente documento (véanse 6.5.2, A.6.4, anexo B y anexo C). Esta estructura permitiría codificar una versión con firma digital de las dos plantillas de las huellas dactilares creadas a partir de minucias utilizando un máximo de 635 bytes. Habida cuenta de que el actual código de barras bidimensional descrito en la norma ILO SID-0002 contiene una segunda copia de determinada información demográfica que ya está impresa en el DIM, actualmente se pueden utilizar un máximo de 686 bytes. Si se eliminara la información duplicada y se sustituyera por el bloque de seguridad del CBEFF, el DIM podría beneficiarse de la seguridad que proporciona la criptografía digital al tiempo que se reducían los datos almacenados en el código de barras, lo que conduciría a que el DIM fuera más fácil de imprimir y leer.

44. Agregar una firma digital al DIM conllevaría claramente importantes ventajas en materia de seguridad, pero la utilización de firmas digitales requiere que los Miembros que quieran utilizarlas se doten de infraestructuras adicionales. En primer lugar, requiere que las autoridades de cada Estado Miembro encargadas de expedir los DIM tengan acceso a su propia clave maestra privada para crear la firma digital y que esta clave se proteja. Para lograrlo, generalmente se guarda en el dispositivo de hardware que se mantiene en una caja fuerte y se conecta al sistema cada varias semanas o meses a fin de crear una clave operativa con firma digital. La clave operativa se utiliza para firmar todos los DIM que se expiden hasta que se cree la nueva clave operativa con la clave maestra. La parte pública de la clave operativa es lo que se distribuye a otros Miembros y lo que les permite verificar la autenticidad de los DIM firmados con esas claves operativas. La seguridad de la clave maestra es fundamental. Si una persona no autorizada la copiara podría falsificar DIM. Se considera que el hardware y el software necesarios para respaldar la seguridad de las firmas digitales agregaría entre 20 000 y 100 000 dólares de los Estados Unidos al coste del sistema de DIM.

45. La segunda parte de la infraestructura adicional consistiría en la creación de un mecanismo a través del que podrían compartirse todas las firmas digitales. Añadir una firma digital a la plantilla de huellas dactilares integrada en un código de barras bidimensional permitiría verificar la autenticidad del código de barras, lo cual requeriría la utilización de la clave pública que corresponda a la clave operativa privada que se utilizó para firmar el código de barras. Por consiguiente, todas las autoridades que quisieran comprobar la autenticidad del DIM tendrían que tener acceso a esas claves. El mismo problema se plantea con los pasaportes electrónicos y, en ese caso, el directorio de claves públicas de la OACI, que es

administrado por la OACI pero de cuyo funcionamiento se ocupa una empresa privada, se utiliza para distribuir las claves públicas.

46. Sería posible colaborar con el directorio de claves públicas de la OACI, pero parece improbable que la utilización de claves públicas se autorice para documentos que no sean pasaportes. También se podrían plantear muchos problemas prácticos, como, por ejemplo, determinar qué organismo gubernamental se encargaría del directorio de claves públicas y la manera en que las claves para los pasaportes electrónicos y los DIM se gestionarían si se tuviera que utilizar el mismo directorio de claves públicas para ambos documentos.

47. Una alternativa sería que la OIT estableciera su propia infraestructura de claves públicas a fin de facilitar el intercambio de claves. Podría tratarse de una infraestructura autónoma o podría gestionarse como una de las funciones de la entidad de coordinación de los centros de coordinación que se examinará a continuación (en la sección A-6). En cualquier caso, tanto el establecimiento de la infraestructura como su mantenimiento conllevarían gastos. Los costos probablemente serían similares a los del directorio de claves públicas de la OACI, que actualmente ascienden [19] a 56 000 dólares de los Estados Unidos como cuota inicial de registro para cada uno de los 39 participantes y 45 000 dólares de los Estados Unidos como cuota anual. Cabe señalar que el costo por participante era más elevado en los primeros años cuando había menos participantes y que, si bien este precio puede parecer elevado, los requisitos de seguridad para el mantenimiento de una infraestructura de claves públicas conllevan gastos importantes. Es probable que la OIT también pudiera beneficiarse de utilizar los mismos servidores y el mismo ancho de banda para acoger la entidad de coordinación de los centros de coordinación y el directorio de claves públicas de la OIT, por lo que estos gastos cubrirían probablemente ambos servicios. Si se adoptara este enfoque, incluso los países que no han ratificado el Convenio núm. 185 necesitarían utilizar los servicios del directorio de claves públicas de la OIT para verificar correctamente los DIM en las fronteras.

Opción A-3. Proyecto de recomendación que se somete a discusión

48. El Consejo de Administración de la OIT podría solicitar a la Oficina que averigüe si los Miembros que han ratificado el Convenio núm. 185 quieren ayudar a sufragar los costes de las infraestructuras para la inclusión de firmas digitales en los DIM. Si hubiera suficientes Miembros interesados, la Oficina tendría que preparar un documento de licitación para contratar a una empresa que creara y mantuviera el directorio de claves públicas de la OIT. Antes de iniciar su propio proceso de licitación, la Oficina podría pedir información a la Secretaría de la OACI sobre la manera en que adquirió y contrató su Directorio de claves públicas. Si no hubiera suficientes Miembros interesados, la Oficina debería solicitar al SC 37 que modificara la norma ISO/IEC 24713-3 para eliminar el bloque de seguridad CBEFF a fin de que aún pudieran utilizarse el resto de las actualizaciones del formato de la plantilla de huellas dactilares.

- **Principales beneficios de la recomendación**

  Los DIM tendrían la misma seguridad digital que los pasaportes electrónicos y, por consiguiente, sería mucho más probable que generarán confianza en el ámbito internacional. Sin una firma digital, tendría que depositarse una excesiva confianza en las investigaciones de los centros de coordinación debido a que sería relativamente fácil falsificar un DIM.

[19] Véase la lista de tarifas de 2014 del directorio de claves públicas de la OACI, disponible en: http://www.icao.int/Security/mrtd/PKD%20Documents/PKDFinanceDocuments/PKDFeeSchedule2014.pdf.

- **Costo de la recomendación y problemas que pueden plantearse**

  Todos los Miembros que expidan DIM (y posiblemente los Miembros que quieran verificar de forma segura la validez de los DIM en las fronteras) tendrían que participar en el directorio de claves públicas y pagar una cuota inicial de registro y una cuota anual. Si sólo pagaran las cuotas los Miembros que expidan DIM, esto equivaldría a las cuotas del directorio de claves públicas de la OACI de 56 000 dólares de los Estados Unidos como cuota de registro inicial y 45 000 dólares de los Estados Unidos anuales. Los Miembros que expiden DIM también tendrían que añadir elementos criptográficos a sus sistemas de expedición de DIM y garantizar una adecuada seguridad física del hardware que contuviera las claves privadas, lo cual ocasionaría un gasto puntual de entre 50 000 y 100 000 dólares de los Estados Unidos. Los Miembros que quisieran verificar los DIM en las fronteras tendrían que garantizar que sus organismos de control de fronteras descargaban las claves públicas de los directorios de claves públicas de la OIT y de la OACI.

A-4. Elaboración de DIM que funcionen con chips

49. Otro elemento que se incluyó en la norma ISO/IEC 24713-3, pero que no se desarrolló de manera detallada, fue la posibilidad de integrar un chip sin contacto en el DIM. El principal problema que se plantea en relación con esta opción es que en el párrafo 9 del artículo 3 del Convenio núm. 185 se estipula que «Todos los datos relativos al marino, que consten en el documento de identidad, deberán ser visibles.» Habida cuenta de que la información que figura en un chip sin contacto sólo resulta visible a través de medios electrónicos, puede entenderse que la utilización de un chip es incompatible con este requisito. La solución consistiría en garantizar que el chip sólo contuviera información acerca del marino que fuera visible en otra parte del documento. De esta forma, el chip sólo contendría una copia de esa información y sería más fácil de leer en la frontera utilizando la infraestructura existente diseñada para los pasaportes electrónicos.

50. Un chip sin contacto que satisficiera exactamente los requisitos del documento núm. 9303 de la OACI se podría leer en las fronteras exactamente con la misma infraestructura que los pasaportes electrónicos tradicionales. En ese caso, el DIM sería un documento de identidad de una sola página con un código de barras bidimensional y un chip sin contacto. Dado que casi ningún organismo de control de fronteras tiene acceso a lectores de códigos de barras, pero que estos organismos tienen acceso a lectores de pasaportes y, en general, también a lectores de pasaportes electrónicos, la zona de lectura mecánica del DIM se podría leer con un lector de pasaportes normal y el chip sin contacto con un lector de pasaportes electrónicos. No sería necesario dotar a los puestos fronterizos de otras infraestructuras y sería mucho más fácil verificar los DIM.

51. Un examen de las últimas versiones de las partes 1 y 3 del volumen 2 del documento núm. 9303 de la OACI [20] pone de relieve que los únicos elementos que obligatoriamente tendrían que almacenarse en un chip sin contacto son el grupo de datos 1, el grupo de datos 2 y los ficheros EF.COM y EF.SOD. Habida cuenta de que el grupo de datos 1 sólo contiene la información que ya está codificada en la zona de lectura mecánica y que el grupo de datos 2 sólo contiene una imagen facial de la persona a la que pertenece el documento (que generalmente se generará a partir de la imagen facial que ya se muestra en la zona visible), estos dos grupos de datos no contienen información alguna que ya no sea visible en el DIM. Además, dado que en el fichero EF.COM sólo figura información sobre

[20] Todas las partes de la versión actual del documento núm. 9303 de la OACI se pueden encontrar en: http://www.icao.int/publications/pages/publication.aspx?docnum=9303.

la versión y la lista de etiquetas para la estructura lógica de datos que contenga los grupos de datos y que en el fichero EF.SOD sólo figura información en relación con la integridad y la autenticidad de los datos (básicamente firmas digitales), en esos ficheros no hay datos sobre el marino. Por consiguiente, parece que podría utilizarse un chip sin contacto con arreglo al documento núm. 9303 de la OACI sin incumplir el artículo 3 del Convenio núm. 185.

52. Si se eligiera esta opción, una de las cuestiones que se plantearían trataría de la conveniencia de que en las firmas digitales que figurarían en el fichero EF.SOD del chip sin contacto del DIM se utilizaran claves privadas que fueran equivalentes a las de las firmas digitales de los pasaportes electrónicos del mismo Miembro. Obviamente, para los funcionarios de fronteras lo más fácil sería que se utilizara la misma infraestructura de claves públicas. Además, si los que expiden DIM y pasaportes electrónicos utilizaran el directorio de claves públicas de la OACI que ya utilizaban para los pasaportes electrónicos no habría costos adicionales, a diferencia de lo que ocurriría con la firma digital para los datos biométricos en el código de barras bidimensional del DIM, que se examinó anteriormente. Por consiguiente, esta opción sería más sencilla y menos costosa, pero requeriría que en cada Estado Miembro la entidad que expide los pasaportes electrónicos y la entidad que expide los DIM colaboraran, habida cuenta de que sólo debería existir una clave maestra privada para cada país que estaría controlada por una de esas entidades, que en la mayor parte de los casos probablemente sería la entidad que expide los pasaportes dado que el directorio de claves públicas de la OACI se centra en los pasaportes electrónicos.

53. Si bien el chip sin contacto haría que el DIM fuera mucho más fácil de verificar, quizá no se trate de la opción preferida por todos los países ya que agregar a cada DIM un chip sin contacto costaría aproximadamente entre 10 y 30 dólares de los Estados Unidos. Por consiguiente, tal como se recomendó en las consultas de septiembre de 2010 [21], que se mencionan en el párrafo 12, el chip sin contacto podría ser optativo, y el código de barras bidimensional y la zona de lectura mecánica seguirían siendo los mecanismos obligatorios para almacenar la información acerca del marino y su plantilla biométrica.

Opción A-4. Proyecto de recomendación que se somete a discusión

54. El Consejo de Administración de la OIT podría solicitar a la Oficina que prepare un proyecto preliminar de texto revisado de los anexos I y II del Convenio núm. 185 en el que los detalles técnicos del código de barras bidimensional y la base electrónica de datos nacional se basen en la norma ISO/IEC 24713-3, y el formato y la presentación del DIM se basen en el documento núm. 9303 de la OACI. En ambos casos, no se incluirían versiones específicas de los documentos de referencia a fin de que pudieran realizarse cambios tecnológicos sin que fuera necesario modificar esos anexos. Asimismo, en los anexos también se describiría un chip sin contacto optativo en el que estén almacenados los grupos de datos 1 y 2 de las partes respectivas del volumen 2 del documento núm. 9303 de la OACI.

55. Las versiones preliminares se presentarían a un órgano marítimo tripartito de la OIT debidamente constituido con miras a la modificación de esos anexos por la CIT con arreglo al artículo 8 del Convenio núm.185.

[21] Los representantes de la gente de mar en las consultas aceptaron que se integrase ese microchip, siempre que los Estados rectores de los puertos tomasen seriamente en consideración la posibilidad de autorizar el descenso a tierra de los titulares de DIM expedidos en virtud del Convenio núm. 185.

56. El Consejo de Administración también podría solicitar a la Oficina que mantenga el contacto con el SC 37 a fin de garantizar que la norma ISO/IEC 24713-3 sigue disponible y se actualiza periódicamente a fin de reflejar los cambios tecnológicos.

- **Principales beneficios de la recomendación**

  Los DIM que llevaran un chip sin contacto optativo serían legibles en la frontera, incluso en los controles fronterizos automáticos, utilizando la misma infraestructura que se utiliza para los pasaportes electrónicos. Además, el chip sin contacto tendría las mismas características de seguridad que un pasaporte electrónico y, por consiguiente, sería más seguro.

- **Costo de la recomendación y problemas que pueden plantearse**

  Los DIM que incluyeran un chip sin contacto costarían aproximadamente entre 10 y 30 dólares de los Estados Unidos más que los DIM equivalentes que no lo incluyeran. Las autoridades de cada Miembro que expidiera DIM con chips sin contacto tendrían que cooperar con las autoridades de ese mismo Estado Miembro que se encarguen de la expedición de pasaportes electrónicos a fin de garantizar que las claves privadas utilizadas para firmar los datos en el chip sin contacto formaban parte del Directorio de claves públicas de la OACI. Un Miembro de la OIT que quisiera utilizar esta característica optativa en el DIM pero que no expidiera pasaportes electrónicos tendría que ponerse en contacto con la OACI a fin saber si el organismo encargado de la expedición de DIM podía participar en el Directorio de claves públicas de la OACI.

A-5. Cambiar los datos biométricos, a saber cambiar la huella digital de un código de barras por una imagen facial

57. Cuando se adoptó el Convenio núm. 185, las normas biométricas se encontraban en una fase temprana de desarrollo y la tecnología biométrica no estaba tan consolidada como lo está ahora. Los Miembros de la OIT que examinaron el texto del Convenio núm. 185 eran conscientes de que para garantizar que se puede comprobar que el marino que presenta un DIM es el titular legítimo de ese documento se necesita algún tipo de verificación biométrica; sin embargo, los detalles técnicos se dejaron para un anexo técnico que podría modificarse a través de un procedimiento acelerado. En el anexo I del Convenio núm. 185 se especifica que los datos que habrán de constar en las páginas previstas en el DIM para los datos se limitarán a una lista de cuestiones que incluyen «*k)* Plantilla biométrica correspondiente a una huella dactilar impresa en forma de números en un código de barras, acorde con una norma que se elaborará posteriormente». La elección de una huella dactilar fue adecuada en 2003, habida cuenta de que el reconocimiento del iris aún tenía protección de patente y básicamente sólo podía realizarlo una empresa, y de que el reconocimiento facial no era lo suficientemente preciso para realizar una verificación segura de la identidad. La decisión de que un código de barras contuviera la huella dactilar también fue apropiada ya que se trataba de unos de los métodos aprobados de almacenaje de datos adicionales que figuraban en el documento núm. 9303 de la OACI.

58. Desde 2003, el código de barras bidimensional se ha eliminado del documento núm. 9303 de la OACI y, tal como se explicó anteriormente en relación con la opción A-4, actualmente el único método autorizado de almacenaje de datos biométricos es el chip sin contacto. La eficacia del reconocimiento facial también ha mejorado mucho y actualmente es lo suficientemente fiable para que en muchos países los viajeros puedan cruzar las fronteras sin intervención de los agentes de control. La infraestructura que se está implantando en las fronteras de todo el mundo se basa en leer datos de las zonas de lectura mecánica de un pasaporte y de un chip sin contacto, y llevar a cabo una comparación, realizada por agentes, de la imagen facial que figura en un chip con el viajero o una

comparación totalmente automática utilizando un sistema automatizado de control fronterizo.

59. Habida cuenta de que esta infraestructura es ampliamente utilizada y de que tiene la confianza de muchos gobiernos, otra posibilidad importante que hay que considerar es si debería actualizarse el anexo I del Convenio núm. 185 a fin de estipular que el elemento biométrico que se tiene que utilizar en el DIM es la imagen facial. En ese caso, el código de barras bidimensional ya no se introduciría en el DIM y se sustituiría por una representación del rostro del marino. A fin de facilitar la verificación, esta representación se almacenaría en un chip sin contacto de la misma estructura lógica de datos que se utiliza en los pasaportes electrónicos (concretamente en el grupo 2 de la estructura lógica de datos). La utilización de una firma digital (véase opción A-3) también tendría que ser obligatoria a fin de crear el fichero EF.SOD exigido como parte de la estructura lógica de datos.

60. Sustituir una huella dactilar almacenada en un código de barras bidimensional por una imagen facial almacenada en un chip sin contacto tiene ventajas. Si se realiza esta sustitución, el DIM que se leerá en los controles fronterizos será exactamente como un pasaporte electrónico, y tendrá una zona de lectura mecánica, un chip sin contacto y una imagen facial para los que se podrá utilizar la misma infraestructura que se utiliza actualmente para los pasaportes electrónicos. Además, el DIM podría utilizarse en un sistema automatizado de control fronterizo al igual que un pasaporte electrónico. Las firmas digitales del DIM podrían ser las mismas que se utilizan en el pasaporte electrónico y el Directorio de claves públicas de la OACI podría utilizarse para distribuir claves públicas. En muchos casos, la huella dactilar podría permitir que la autoridad que expide los pasaportes electrónicos en un país también expidiera los DIM, lo cual conllevaría un ahorro significativo ya que se podría utilizar el mismo software y el mismo hardware para expedir ambos documentos, con la única diferencia de que el pasaporte electrónico se imprime como un libro y el DIM sólo tiene una página. Esto también haría que si se utilizaran las mismas claves para los DIM que para los pasaportes electrónicos ya no fuera necesario pagar otro directorio de claves públicas, ya que la suscripción al Directorio de la OACI ya estaría costeada por la autoridad encargada de la expedición de pasaportes electrónicos. Asimismo, la OIT podría poner fin al programa de pruebas de interoperabilidad de los sistemas de huellas dactilares y ahorrarse lo que cuesta este programa, habida cuenta de que ya existe un programa bien establecido de interoperabilidad de los pasaportes electrónicos y de que gracias a los sistemas automatizados de control fronterizo el uso internacional de las imágenes faciales para la correspondencia biométrica también está bien establecido en muchos países.

61. No obstante, introducir esta modificación en los DIM también podría acarrear problemas. El primer problema radicaría en que este importante cambio implicaría que los Miembros de la OIT que ya han instalado sistemas de expedición de DIM o que estén adquiriendo este tipo de sistemas tendrían que introducir modificaciones sustanciales en sus sistemas o adquirir sistemas totalmente nuevos compatibles con la expedición de pasaportes electrónicos. A fin de minimizar esas dificultades sería necesario informar de que se va a realizar un cambio pero esperar un tiempo antes realizarlo, y además establecer un período de transición adicional para los Miembros que ya hayan instalado un sistema de expedición de DIM. El segundo problema consistiría en que sólo los Miembros que ya utilizan pasaportes electrónicos (que cada vez son más) podrían aprovechar las ventajas de suprimir el sistema de DIM y utilizar el sistema de pasaportes electrónicos existente, a lo que habría que añadir que también serían necesarias ciertas negociaciones entre la autoridad encargada de la expedición de DIM y la autoridad encargada de la expedición de pasaportes electrónicos, lo cual puede que no sea fácil para algunos Miembros. El tercer problema radicaría en que debido a la incorporación de un chip sin contacto el costo de fabricación de cada DIM aumentaría un poco (aproximadamente entre 10 y 30 dólares de los Estados Unidos por DIM).

62. Existe una cuestión jurídica que también tendría que examinarse. El apartado *b)* del párrafo 8 del artículo 3 del Convenio núm. 185 prevé que es necesario «que los datos biométricos sean visibles en el documento, y no puedan reconstituirse a partir de la plantilla o de otras representaciones». La imagen facial ha de ser claramente visible en el documento ya que el apartado *f)* del párrafo 7 de este artículo estipula que en el documento debe haber una «fotografía digital u original». La cuestión que se plantea es saber si una imagen facial también puede satisfacer la exigencia de que los datos biométricos «no puedan reconstituirse a partir de la plantilla o de otras representaciones». Actualmente, en el DIM se utiliza una plantilla a partir de minucias dactilares. Si bien es posible aplicar ingeniería inversa a la plantilla creada a partir de minucias a fin de crear una huella dactilar sintética que sea muy similar y se ajuste a la huella dactilar del marino, no se tratará de una representación perfecta de esa huella dactilar debido a que faltarán los poros y las cicatrices y otra información que no tiene relación con las minucias y que hará que las diferencias sean fácilmente detectables por una persona experta o por un sistema biométrico con capacidad de «detección en vivo». Una imagen facial, considerada de la misma forma que una plantilla de huellas dactilares, es una representación bidimensional del rostro de un marino y aunque se puede imprimir una imagen muy similar a ese rostro, no se puede generar una adecuada representación tridimensional del rostro del marino. Por consiguiente, un observador humano o un sistema biométrico con capacidad de «detección en vivo» podrían distinguir una máscara impresa del rostro real del marino. Por consiguiente, es importante que antes de aceptar la opción de sustituir una huella dactilar en un código de barras por una imagen facial en un chip sin contacto se examine si una imagen facial puede satisfacer los requisitos del apartado *b)* del párrafo 8 del artículo 3 del Convenio núm. 185.

Opción A-5. Proyecto de recomendación que se somete a discusión

63. El Consejo de Administración de la OIT podría solicitar a la Oficina que prepare un proyecto preliminar de texto revisado de los anexos I y II del Convenio núm. 185 en el que los datos biométricos se cambien, a saber en el que se cambie una plantilla de huellas dactilares integrada en un código de barras bidimensional por una imagen facial que se extraería de una fotografía del marino y se almacenaría en un chip sin contacto. La base electrónica de datos nacional contendría las claves públicas necesarias para verificar las firmas digitales que se definieran para el chip sin contacto en el documento núm. 9303 de la OACI. Además, se podrían suprimir todas las referencias a normas técnicas distintas al documento núm. 9303 de la OACI dado que en el documento núm. 9303 de la OACI ya se haría referencia a todas las normas pertinentes de la ISO.

64. Las versiones provisionales se someterían a un órgano marítimo tripartito de la OIT debidamente constituido con miras a que la CIT modificara esos anexos de conformidad con el artículo 8 del Convenio núm. 185.

65. Habida cuenta de la importancia de esos cambios, también se redactaría y se distribuiría junto con el proyecto de texto de revisión de los anexos un documento de orientación en el que se explicaría la repercusión que tendrían los cambios y la necesidad de que las autoridades encargadas de expedir DIM de un país colaboraran con las autoridades encargadas de expedir pasaportes electrónicos de ese mismo país. Debido a la importancia de los cambios probablemente debería establecerse un largo período de transición a fin de que los Miembros que estuvieran expidiendo DIM pudieran introducir los cambios. Además, habida cuenta de la necesidad de dar el apoyo al sistema de expedición de DIM durante el período de transición, esta recomendación también se combinaría con otra ronda de pruebas de interoperabilidad de los sistemas de huellas dactilares, tal como se examinó en la sección A-2.

- **Principales beneficios de la recomendación**

  La autentificación de los DIM por parte de los funcionarios encargados de los visados, los agentes de fronteras y otras personas encargadas de verificar los DIM en todo el mundo se simplificaría debido a que para los DIM se utilizaría la misma infraestructura y exactamente la misma seguridad que para los pasaportes electrónicos. Esto tendría la ventaja añadida de hacer que los DIM fueran aceptados más fácilmente como documento de identidad por la mayor parte de los países. Los precios de los sistemas de expedición se reducirían mucho si también fueran costeados por la autoridad encargada de la expedición de pasaportes electrónicos de cada Miembro y se suprimiría el gasto que implica mantener un sistema independiente de distribución de claves públicas. Además, también se eliminaría el coste de las pruebas de interoperabilidad en materia de huellas dactilares, con la excepción de una ronda final de pruebas para respaldar el sistema de expedición de DIM durante el período de transición.

- **Costo de la recomendación y problemas que pueden plantearse**

  La fabricación de cada DIM costaría aproximadamente entre 10 y 30 dólares de los Estados Unidos más que antes. Muchas de las ventajas y ahorros asociados a esta opción sólo se podrían aprovechar si la autoridad encargada de expedir DIM de cada Miembro de la OIT cooperara con la autoridad encargada de expedir pasaportes electrónicos de ese mismo Miembro. Esto podría representar un problema para algunos países. Además, los países que ya han instalado un sistema de DIM tendrían muchos gastos debido a que después del período de transición tendrían que introducir cambios en ese sistema, si la CIT decidiera aprobarlos.

A-6. Establecimiento de una entidad de coordinación de centros de coordinación

66. Asimismo, el Convenio exige el establecimiento de una base electrónica de datos y un centro de coordinación nacionales para el intercambio y la verificación de la información, con miras a que las autoridades competentes de todos los Miembros de la OIT verifiquen la autenticidad de los DIM, validación de debería poder realizarse en cualquier momento. Sin embargo, también se debe respetar el derecho de la gente de mar a la privacidad y a la protección de los datos.

67. Las siguientes disposiciones del artículo 4 del Convenio núm. 185 establecen las exigencias funcionales clave en relación con la base de datos electrónica y el centro de coordinación nacionales:

> 1. Todo Miembro velará por que se conserve en una base electrónica de datos constancia de cada documento de la gente de mar que haya sido expedido, suspendido o retirado. …
>
> 2. En cada referencia figurarán solamente los datos que resulten esenciales para verificar el documento de identidad o la condición del marino, sin menoscabo del derecho a la privacidad de este último y con arreglo a todas las disposiciones aplicables en materia de protección de datos. …
>
> …
>
> 4. Cada Miembro designará un centro permanente de coordinación encargado de responder a las solicitudes de información cursadas por los servicios de inmigración u otras autoridades competentes de todos los Miembros de la Organización, en relación con la autenticidad y la validez de los documentos de identidad de la gente de mar expedidos por la autoridad de que se trate. …

5. Los servicios de inmigración u otras autoridades competentes de los Estados Miembros de la Organización deberán tener acceso, de manera inmediata y en todo momento, a los datos mencionados en el párrafo 2 *supra*, ya sea por medios electrónicos, o a través del centro de coordinación mencionado en el párrafo 4 *supra*.

68. Si las bases electrónicas de datos nacionales que se describen en el Convenio núm. 185 se quieren usar de manera eficaz, las autoridades competentes pertinentes deben poder acceder a ellas de manera adecuada. Si, por ejemplo, un agente de fronteras tiene dudas acerca de la autenticidad del DIM de un marino tendrá que poder ponerse en contacto con el centro de coordinación pertinente a fin de validar ese DIM. El anexo I del Convenio núm. 185 estipula que en el DIM debe figurar el número de teléfono, la dirección de correo electrónico y el sitio web de los enlaces con el centro de coordinación. Sin embargo, cabe tener en cuenta que si un funcionario de fronteras envía un correo electrónico el marino deberá permanecer en la frontera durante el tiempo que tarde en recibirse la respuesta. Esto plantea una serie de problemas prácticos. Además, si el agente de fronteras llama a un número de teléfono pueden plantearse problemas debido al idioma. Si el agente se conecta a Internet y accede al sitio web del centro de coordinación podrá obtener cierta información, pero se plantea la cuestión de cuánta información ha de poder obtener un usuario anónimo a través de un sitio web, habida cuenta de que también debe protegerse el derecho a la privacidad del marino. También existe el problema general de que si un agente de fronteras duda de la autenticidad de un determinado DIM, quizá tampoco dé crédito a la información que reciba a través de un número de teléfono, una dirección de correo electrónico o un sitio web que sólo conozca porque figuran en el DIM del marino.

69. Asimismo, el párrafo 4 del artículo 4 del Convenio también estipula que «Los datos relativos al centro de coordinación permanente se pondrán en conocimiento de la Oficina Internacional del Trabajo, la cual llevará una lista que se comunicará a todos los Miembros de la Organización». De esta forma, los funcionarios de fronteras u otros agentes de la autoridad competente sabrían cómo ponerse en contacto con el centro de coordinación pertinente para verificar un DIM. Sin embargo, en la práctica, se plantearía el problema de que llevaría tiempo elaborar una lista con los números de teléfono, los sitios web y las direcciones de correo electrónico de los centros de coordinación de todos los Miembros de la OIT que han ratificado el Convenio núm. 185. Además, sería poco probable que esa lista estuviera a disposición de todos los funcionarios de fronteras de todo el mundo y, concretamente, de todos los puertos en los que los marinos pueden presentar sus DIM.

70. La mejor manera de conseguir que un sistema de este tipo funcione sería estableciendo una entidad de coordinación de los centros de coordinación que pueda responder a las consultas en relación con la autenticidad y validez de los DIM que puedan realizar los agentes de fronteras, los funcionarios encargados de los visados u otras autoridades competentes. Lo más conveniente sería que esta entidad de coordinación estuviera en Internet, ya que de esta forma se podría consultar fácilmente en todo momento y en diferentes idiomas, y se cubrirían mejor las necesidades de las autoridades competentes de distintos países. En consecuencia, la OIT proporcionaría los datos de contacto de la entidad de coordinación de los centros de coordinación a todos sus Miembros, a saber el enlace con un solo sitio web y un solo número de teléfono. En virtud del artículo 4 del Convenio, cada centro de coordinación nacional [22] será responsable de la exactitud de la información proporcionada

[22] Si bien el párrafo 4 del artículo 4 (titulado «Base electrónica de datos nacional») del Convenio núm. 185 no estipula expresamente que el «centro permanente de coordinación» que tiene que ser establecido por cada uno de los países que ratifiquen el Convenio debe estar situado en el país interesado, esto se desprende de los trabajos preparatorios del Convenio en relación con los centros de coordinación y está en consonancia con el supuesto básico de que las autoridades nacionales son las que están en mejor posición para proporcionar información de primera mano sobre sus nacionales o residentes permanentes.

por la entidad de coordinación en relación con los datos de los DIM almacenados en su base de datos electrónica nacional y tendrá que estar disponible de manera permanente para responder a todas las preguntas a las que no dé respuesta la entidad de coordinación de los centros de coordinación. Sin embargo, si se estableciera la entidad de coordinación se aligeraría en gran medida la carga del centro nacional de coordinación en lo que respecta a proporcionar respuestas inmediatas a cualquier agente del mundo y en cualquier momento y en condiciones en las que se respete el derecho a la privacidad del marino interesado.

71. Existen dos opciones básicas en relación con el establecimiento de una entidad de coordinación de los centros de coordinación, a saber:

a) un servidor central conectado a los servidores de los Miembros con cuyo software se pueda acceder a las bases electrónicas de datos nacionales. Ese servidor central recibiría una solicitud de información de las autoridades competentes y después realizaría su propia solicitud de información al servidor pertinente del Estado Miembro que corresponda, tras lo cual respondería a la solicitud de información de la autoridad competente sobre la base de la respuesta que hubiera recibido de la base electrónica de datos del Estado Miembro. Este método exigiría una conectividad continua entre el servidor central y cada base electrónica de datos nacional; o

b) un servidor central que contenga copia de la información que figura en las bases electrónicas de datos nacionales de todos los Miembros y que reciba cada día y cada hora actualizaciones de las autoridades encargadas de la expedición de DIM a medida en que esas autoridades introduzcan cambios en sus bases electrónicas de datos nacionales. Este servidor recibiría las solicitudes de información a través de su sitio Web y respondería a ellas sobre la base de su propia copia de la base electrónica de datos nacional pertinente. Este método sólo requeriría una conectividad periódica con cada base electrónica de datos nacional, pero se correría el riesgo de que la información estuviera ligeramente desfasada, y si el mismo día en que se había expedido su DIM se tuviera que verificar la identidad de un marino en la frontera puede que la información no estuviera disponible. Estos inconvenientes no se plantearían si el sitio Web dispusiera de una conexión a Internet que funcionara plenamente, ya que en ese caso se podría esperar que las actualizaciones se realizaran al mismo tiempo que los cambios en la base electrónica de datos nacional. Si se utilizara este método, sería necesario que el servidor de base de datos de la entidad de coordinación de los centros de coordinación fuera seguro, ya que en él se almacenaría directamente información sobre todos los marinos que tengan un DIM.

72. El costo de establecer un entidad de coordinación de los centros de coordinación sería muy elevado (probablemente entre 1 y 2 millones de dólares de los Estados Unidos para desarrollar el software y establecer la infraestructura inicial) y los costos operativos ordinarios también serían considerables (probablemente varios cientos de miles de dólares cada año) debido a que habría que tener gente trabajando 24 horas al día 365 días al año e instalar una infraestructura de seguridad muy potente a fin de proteger los datos de la gente de mar y asegurarse de que sólo se aceptaban las solicitudes de información que procedieran de entidades autorizadas.

73. De hecho, encontrar un equilibrio entre la protección de los datos de la gente de mar y su derecho a la privacidad y la necesidad de responder a las legítimas solicitudes de información es un factor crítico para establecer una entidad de coordinación de los centros de coordinación. En la norma ISO/IEC 24713-3 se examinan algunos de esos factores y se proponen una serie de posibles tipos de solicitudes de información en función del nivel de confianza entre el expedidor del DIM y el país del que proceda la solicitud de información. El contenido exacto de cada posible solicitud de información y de la respuesta de la entidad de coordinación dependería de algunas de las otras propuestas que figuran en este

documento, que implican posibles cambios en los anexos I y II del Convenio núm. 185. La decisión de usar firmas digitales (véase opción A-3.), en particular, tendría un impacto significativo sobre qué información se intercambiaría y cómo se protegería esa información. Por consiguiente, las características de cada solicitud de información y de cada respuesta tendrían que determinarse después de que se hubiera resuelto la cuestión de los otros cambios que se podrían introducir en el DIM.

74. No obstante, a pesar de los costos, disponer de una entidad de coordinación de los centros de coordinación puede tener muchas ventajas. Si se decidiera incluir firmas digitales en los DIM, la entidad de coordinación también podría distribuir las claves públicas necesarias para validar los DIM, al igual que el directorio de claves públicas de la OACI hace con los pasaportes digitales. En ese caso, el costo total de establecer y mantener la entidad de coordinación podría incluirse probablemente en el costo de mantener un directorio de claves públicas, tal como se examinó en la opción A-3. Concretamente, esos costos ascenderían a alrededor de 56 000 dólares de los Estados Unidos por Miembro participante como cuota de registro inicial y 45 000 dólares de los Estados Unidos anuales por Miembro.

Opción A-6. Proyecto de recomendación que se somete a discusión

75. El Consejo de Administración de la OIT podría solicitar a la Oficina que averigüe si los Miembros que han ratificado el Convenio núm. 185 quieren dar apoyo financiero a una entidad de coordinación que sirva para respaldar a sus centros nacionales de coordinación. La pregunta debería ir acompañada de una explicación de las propuestas de mecanismos operativos para la entidad de coordinación de los centros de coordinación (servidor central conectado a las bases de datos electrónicas nacionales, servidor central que almacene copias de las bases electrónicas de datos nacionales, y posible apoyo a la distribución de claves para DIM con firma digital) basada en la compatibilidad con otros proyectos de recomendaciones que se puedan seleccionar para ser implementados entre las opciones que figuran en este documento. Si hubiera un número suficiente de Miembros interesados, la Oficina podría preparar un documento de licitación para contratar una empresa de confianza que cree y acoja la entidad de coordinación de los centros de coordinación.

- **Principales beneficios de la recomendación**

  La autentificación de los DIM por parte de las autoridades fronterizas y otras autoridades de todo el mundo se simplificaría y se reducirían considerablemente los gastos y los esfuerzos que tienen que realizar los Miembros para mantener sus centros de coordinación nacionales y proteger el derecho a la privacidad de los marinos y la seguridad de sus datos. Los servicios que proporcionan los centros de coordinación nacionales y los tipos de solicitudes de información que se les presentan, que difieren de un país a otro, podrían normalizarse y se obtendría la misma información utilizando un único mecanismo de acceso para todos los Miembros que han ratificado el Convenio núm. 185.

- **Costo de la recomendación y problemas que pueden plantearse**

  La Oficina tendría que organizar una licitación a fin de establecer el mecanismo de gestión cuotas. La participación en la entidad de coordinación de centros de coordinación supondría un costo inicial y un costo anual para cada Miembro que ha ratificado el Convenio núm. 185. Sobre la base de los costes de funcionamiento del Directorio de claves públicas de la OACI, el costo por Miembro podría ascender a alrededor de 56 000 dólares de los Estados Unidos para el registro inicial y 45 000 dólares de los Estados Unidos anuales.

A-7. Colaboración entre los Miembros para establecer sistemas de expedición de DIM

76. Muchos de los países con economías menos desarrolladas no disponen de los conocimientos técnicos para crear sus propios sistemas de DIM ni de los fondos necesarios para comprar un sistema de este tipo a un proveedor comercial. Para los países que cuentan con pocos marinos, el costo por marino del cumplimiento de todas las exigencias del Convenio núm. 185 puede ser muy elevado. Un sistema completo de DIM generalmente cuesta entre unos cientos de miles y unos millones de dólares de los Estados Unidos, dependiendo del número de marinos y de puntos de expedición y de registro. Incluso después de que se haya desarrollado o comprado el sistema, hay costes adicionales de formación de personal y de funcionamiento regular, que incluyen no sólo los servicios para registrar a los marinos sino también el mantenimiento de un centro de coordinación y una base electrónica de datos nacionales que estén disponibles de forma continua. Para muchos Miembros de la OIT, estos costes y la complejidad técnica asociada a la creación y mantenimiento de un sistema de este tipo dificultan considerablemente la ratificación del Convenio núm. 185.

77. Hay algunas opciones que permitirían que los países colaboraran a fin de reducir esos costes, tanto en materia técnica como en materia financiera. Los costes se reducirían especialmente si los países más grandes, que disponen de infraestructuras de TI más sofisticadas, colaboraran con los países más pequeños. Habida cuenta de que se pueden tener en cuenta diversas opciones, a diferencia de lo que se hizo en las secciones anteriores, en esta sección las opciones se presentan para que sean examinadas y no se propone ninguna recomendación. Es posible que varias opciones diferentes puedan utilizarse al mismo tiempo.

78. **Opción 1 – Un Miembro dona su propio sistema de DIM:** Podría ponerse copia gratuita del software de un sistema de DIM desarrollado por un país a disposición de otros países. En los países que recibieran ese software se reduciría mucho el costo de aplicar el Convenio núm. 185. Si se realizara una evaluación independiente en el primer país que usara ese software, las siguientes evaluaciones independientes que se realizaran en todos los otros países que usaran el mismo software serían mucho más simples y sería más probable que su resultado fuera favorable. Esta opción requiere que un Miembro de la OIT, tanto si ha ratificado el Convenio núm. 185 como si no lo ha ratificado, esté dispuesto a crear un sistema y a distribuirlo gratuitamente a los otros Miembros.

79. **Opción 2 – Un sistema de DIM regional y compartido:** Varios países podrían trabajar juntos para crear un sistema de expedición de DIM, un centro de coordinación y una base electrónica de datos regionales. Ese sistema podría utilizarse para expedir DIM para todos esos países, los cuales seguirían registrando a sus propios marinos y tomando decisiones acerca de si dichos marinos cumplen con los requisitos para el registro, pero utilizarían un sistema de expedición con base en la Web ubicado en uno de los países y todas las impresiones de documentos se realizarían en la instalación central en la que estaría ubicado el sistema. Además, ese sistema almacenaría las bases electrónicas de datos de esos países en un depósito de datos independiente que estaría disponible para los centros de coordinación nacionales. Esto permitiría que varios países compartieran el costo del sistema de expedición de DIM y de las bases electrónicas de datos nacionales, reduciéndose de esta forma el costo para cada país. Una gran parte de la evaluación independiente se llevaría a cabo en el emplazamiento central, y sólo sería necesario controlar un número limitado de cuestiones en cada lugar de registro de cada país, reduciéndose de esta forma el tiempo y el costo de las evaluaciones independientes para cada uno de los países participantes.

80. Opción 3 – Desarrollo independiente, financiado por donantes, de un sistema de expedición de DIM con derechos de propiedad intelectual exclusivos: Un país donante o un grupo de países donantes podrían aportar fondos suficientes (probablemente entre 1 y 3 millones de dólares de los Estados Unidos) para costear un sistema de DIM que incluyera el registro, la impresión, la supervisión de existencias, la base electrónica de datos nacional y todos los otros elementos del sistema desarrollados desde cero por una tercera parte. Este sistema se diseñaría para trabajar con componentes de hardware estándar, tales como computadoras e impresoras personales, etc. La propiedad intelectual de este software podría transferirse después a la OIT, que de forma gratuita la pondría a disposición de todos los países que ratifiquen el Convenio núm. 185. Podría realizarse una evaluación independiente de todos los elementos del software de ese sistema utilizando una copia del sistema configurado en la OIT en el marco del procedimiento de aceptación del software que proporcionó el programador independiente. Utilizando esta evaluación como base, todas las evaluaciones posteriores de otras copias del software que realicen determinados países deberían ser mucho más simples y más rápidas y sería más probable que su resultado fuera favorable en comparación con una evaluación independiente que empezara desde cero con un sistema desconocido. El resultado final sería conseguir que la aplicación del Convenio núm. 185 fuera más simple y más barata para todos los países que se beneficiaran de la versión de la OIT del sistema de DIM.

81. Opción 4 – Licitación mundial y compartida: una organización internacional como la OIT, conjuntamente con uno o más países con conocimientos especializados en sistemas de TI y de licitaciones en materia de TI, podría organizar un proceso de licitación mundial de componentes de un sistema de DIM, que incluyera los puestos de registro, el software de expedición central, los dispositivos de huellas dactilares, las impresoras, las tarjetas, etc. Esos elementos de software y hardware podrían ponerse a disposición de todos los países interesados en aplicar el Convenio núm. 185 utilizando una lista de precios fijos propuestos por el adjudicatario o los adjudicatarios del proceso de licitación. Si se pudiera garantizar que para dotarse de equipos todos o una amplia mayoría de los países que aplican el Convenio núm. 185 adquirirían los productos que figuraran en esa lista, se economizaría mucho debido a que se trataría de productos mucho más baratos que los que cada país podría adquirir por su propia cuenta. Asimismo, las evaluaciones independientes se simplificarían debido a que los componentes de hardware y software que se evaluarían serían casi idénticos de un país a otro. Sin embargo, si no se pudiera garantizar que la mayor parte de los países adquirirían los productos que figuraran en esa lista no se lograrían ventajas significativas en relación con el aprovisionamiento individual realizado por los diversos países, excepto en lo que respecta a simplificar su propio proceso de licitación.

B. Opciones para los Miembros que no han ratificado el Convenio núm. 185 en relación con el uso de DIM expedidos en virtud de dicho Convenio

82. En la sección siguiente se examinan tres opciones para abordar la situación de los Miembros que no han ratificado el Convenio núm. 185 pero pueden desear considerar la posibilidad de cooperar en su aplicación para facilitar el acceso de la gente de mar a su territorio con fines de disfrute del permiso para bajar a tierra, tránsito o asuntos conexos. Se trata de las siguientes opciones:

B-1. Usar los DIM expedidos en virtud del Convenio núm. 185 para tomar decisiones en relación con la admisión de marinos.

B-2. Verificar la identidad de los marinos.

B-3. Autentificar los DIM.

B-1. Usar los DIM expedidos en virtud del Convenio núm. 185 para tomar decisiones en relación con la admisión de marinos

83. Es importante señalar que los países no signatarios del Convenio núm. 185 ya pueden utilizar también el sistema de identificación previsto en dicho Convenio, y que todos los Miembros de la OIT han de poder aprovechar muchas de las ventajas que ofrece este sistema. Concretamente, todos los Miembros de la OIT:

a) reciben una lista de los centros de coordinación nacionales abiertos en los Estados Miembros signatarios, que sus servicios de inmigración y demás autoridades competentes tendrán el derecho de consultar para verificar la autenticidad y validez de los DIM expedidos en el país del centro de coordinación considerado (párrafo 4 del artículo 4);

b) obtienen, de los centros de coordinación o de las bases de datos nacionales, datos esenciales para verificar los DIM o la condición jurídica de los marinos (sin vulnerar el derecho a la privacidad y a la protección de datos personales) (párrafo 5 del artículo 4), y

c) tienen acceso a una lista actualizada de los Miembros cuyos procesos y procedimientos de expedición se ajustan a los requisitos mínimos del Convenio (párrafo 7 del artículo 5).

84. Si para tomar una decisión acerca de permitir que un marino acceda a su territorio con fines de disfrute de un permiso para bajar a tierra, tránsito, reembarco en otro buque, o repatriación, un Miembro de la OIT que no ha ratificado el Convenio núm. 185 quiere examinar debidamente el DIM de ese marino expedido con arreglo al Convenio se beneficiará, tal como se señaló anteriormente, tanto de la seguridad del documento como de la seguridad del sistema de expedición, que habrá sido objeto de una evaluación independiente.

85. Existen dos situaciones diferentes en las que, al interactuar con un marino, un Estado Miembro que no ha ratificado el Convenio puede aprovechar la mejora de la seguridad de los DIM. La primera situación se produce cuando un marino llega a la frontera y quiere embarcar en un buque o desembarcar de un buque o disfrutar del permiso para bajar a tierra en un puerto. Aunque el Estado Miembro no haya ratificado el Convenio núm. 185, puede tener la obligación de dejar acceder a su territorio a la gente de mar en virtud de otros convenios de la OIT como el Convenio núm. 108 o el MLC, 2006, o en virtud del Convenio FAL de la OMI. En ese caso, sería beneficioso para el Miembro que no ha ratificado el Convenio poder verificar de manera más segura la identidad de los marinos. La segunda situación se plantea cuando los marinos se presentan en una embajada o un consulado para solicitar un visado. Actualmente, algunos Miembros exigen que los marinos dispongan de un visado para entrar en su territorio con fines de tránsito o reembarco en otro buque y algunos países que no han ratificado el Convenio también exigen que los marinos dispongan de un visado para disfrutar del permiso para bajar a tierra. En ese caso, también sería útil que el Miembro dispusiera de un sistema más seguro para identificar a los marinos y verificar si tienen derecho a solicitar un visado debido a su trabajo como marinos. Por consiguiente, como parte del proceso de solicitud de un visado deberían validarse los DIM y debería verificarse la identidad de los marinos.

86. Las ventajas antes mencionadas serían, por supuesto, menores para los Miembros que no dispusieran de los dispositivos necesarios para leer la información que contienen los DIM expedidos con arreglo al Convenio núm. 185. EL DIM es un documento de lectura mecánica de conformidad con las normas previstas en el documento núm. 9303 de la OACI, y lo que figura en su zona de lectura mecánica puede ser leído por cualquier lector

de pasaportes que cumpla con la normativa de la OACI. Sin embargo, la plantilla biométrica que requiere el párrafo 8 del artículo 3 del Convenio está almacenada en un código de barras bidimensional. Si una autoridad de control de fronteras o de inmigración desea verificar la huella digital de un marino necesitará disponer de los dispositivos necesarios para leer códigos de barras y para captar y cotejar las huellas dactilares. Pueden examinarse dos opciones en lo que respecta a aumentar la utilidad de los DIM en países que no han ratificado el Convenio núm. 185:

- **Opción 1 – Desarrollo de un DIM optativo que funcione con chips:** Tal como se examinó en la sección A-4, sería posible modificar los anexos I y II del Convenio núm. 185 para incluir un microchip sin contacto optativo que contenga toda la información que ya figura en el DIM. Esto permitiría leer el DIM con un lector de pasaportes electrónicos estándar y facilitaría la lectura por parte de los países que no han ratificado el Convenio de los DIM que los marinos presenten en la frontera. Esta posibilidad se debatió en las consultas tripartitas sobre el Convenio núm. 185 que se realizaron en septiembre de 2010, a las que se hace referencia en el párrafo 12. En esas consultas se convino en la procedencia de elaborar una norma para la incorporación facultativa en el DIM de un microchip que contenga toda la información ya incorporada al DIM. Los representantes de la gente de mar en las consultas aceptaron que se integrase ese microchip, siempre que los Estados rectores de los puertos tomasen seriamente en consideración la posibilidad de autorizar el descenso a tierra de los titulares de DIM expedidos en virtud del Convenio núm. 185.

- **Opción 2 – Cambiar los datos biométricos, a saber cambiar la huella digital en un código de barras por una imagen facial:** Esta opción, que se examina en la sección A-5, aportaría todos los beneficios de añadir un microchip optativo a los DIM, y también permitiría que los Miembros que no han ratificado el Convenio verificaran la identidad de los marinos a través del reconocimiento facial (realizado por agentes o por un sistema automatizado de control fronterizo) y que se comprobara la validez de los DIM utilizando el sistema de firmas digitales con claves públicas distribuido a través del Directorio de claves públicas de la OACI que ya se utiliza para verificar los pasaportes electrónicos. Esto haría que los sistemas de DIM fueran completamente interoperables con los sistemas que se utilizan actualmente para los pasaportes electrónicos y no sería necesario disponer de otra infraestructura o que los Miembros que no han ratificado el Convenio realizaran esfuerzos para aprovechar la seguridad adicional que ofrecerían los DIM.

87. Los Miembros que no han ratificado el Convenio quizá también desearían hacer uso de la posibilidad de comprobar de forma independiente la autenticidad de un DIM poniéndose en contacto con el centro de coordinación nacional del Miembro que lo ha expedido. Para ello se tendría que definir una forma de ponerse en contacto con los centros de coordinación existentes y habría que disponer la infraestructura necesaria para permitir esa comunicación cuando se autentifique un DIM. Habida cuenta de que el párrafo 3 del artículo 6 del Convenio estipula que la comprobación de la identidad del marino deberá «efectuarse a la mayor brevedad, siempre que las autoridades competentes hayan recibido con tiempo suficiente el aviso de llegada del titular», los Miembros podrían ponerse en contacto con el centro nacional de coordinación para la gente de mar cuando se transmita la información acerca de la llegada del titular del DIM, en lugar de cuando el marino solicite poder disfrutar de su permiso para bajar a tierra en el puerto. Esto podría reducir las dificultades que supondría dotar infraestructuras de comunicación adecuadas a todos los puertos y puestos fronterizos, pero requeriría más coordinación en lo que respecta a recibir los avisos de llegada y tramitarlos.

88. Si no se tomara la decisión de cambiar la huella digital en un código de barras por una imagen facial (o en el período transitorio antes de que esta decisión se haga efectiva), los Miembros que no han ratificado el Convenio necesitarían un mecanismo para leer los DIM

y comprobar la identidad de los marinos, así como un mecanismo para ponerse en contacto con los centros nacionales de coordinación a fin comprobar la validez de los DIM. A continuación se examinan más detalladamente algunas opciones técnicas para ejecutar estas acciones.

B-2. Verificar la identidad de los marinos

89. Todo Miembro que desee comprobar la identidad de los marinos en un puerto u otro punto fronterizo necesita disponer de ciertas infraestructuras. El mínimo absoluto sería disponer de un lector de pasaportes estándar que pueda leer la zona de lectura mecánica de los DIM actuales. Este lector permite leer automáticamente la información que figura en el DIM, pero no permite verificar la identidad de un marino ni autentificar el DIM. A fin de verificar la identidad de un marino se necesita un mecanismo para leer y verificar los datos biométricos. Para leer los DIM actuales se necesita un lector de códigos de barras, un sensor de huellas dactilares interoperable y el software correspondiente para cotejar las huellas dactilares. El coste total de un lector de códigos de barras y de un producto para las huellas dactilares oscila entre 400 y 1 200 dólares de los Estados Unidos, dependiendo del hardware que se elija. Estos materiales pueden integrarse en una aplicación independiente de una computadora de un punto de control secundario (sencillo y económico), en el software existente de la inspección principal de cada puesto fronterizo (posiblemente bastante caro) o en una unidad móvil (práctico pero más complicado). Resulta difícil calcular los costes de integración del software, pero el desarrollo de una simple aplicación para una computadora independiente de un punto de control secundario debería costar menos de 10 000 dólares de los Estados Unidos.

90. La idea de enviar a los marinos (cuya condición de marinos hay que verificar antes de permitirles cruzar la frontera) a un punto de control secundario con una aplicación independiente en materia de verificación tiene sentido en la mayor parte de los puestos fronterizos, ya que en comparación con el número total de personas que cruzan una frontera el número de marinos es reducido. Sin embargo, en algunos puertos puede que resulte insuficiente disponer de un solo punto fijo para todos los marinos cuya identidad hay que verificar y podría ser más útil disponer de dispositivos móviles que puedan llevarse a bordo de los buques. Dado que en el mercado ya hay muchos escáneres móviles de huellas dactilares y documentos, no sería difícil fabricar dispositivos móviles para los DIM. Sin embargo, hasta ahora no ha habido suficiente demanda para que alguno de los fabricantes de dispositivos móviles introduzca los cambios necesarios para poder utilizarlos con los DIM.

91. Un Miembro que no haya ratificado el Convenio núm. 185 puede decidir dar preferencia a los marinos que tengan DIM con chip incorporado, ya que estos DIM pueden verificarse utilizando un lector de pasaportes electrónicos estándar y no requieren un lector de códigos de barras independiente, lo que llevaría a esos Miembros a ahorrar entre 200 y 400 dólares de los Estados Unidos por punto de verificación.

B-3. Autentificar los DIM

92. Una vez que se haya comprobado que un marino es el titular legítimo de un DIM, aún quedará pendiente la cuestión de si ese DIM es un documento auténtico. Según el sistema actual de DIM, la única forma de comprobar que ese DIM es auténtico es poniéndose en contacto con el centro de coordinación del Estado Miembro que lo ha expedido. Si bien un DIM contiene información de contacto con el centro nacional de coordinación correspondiente, un documento falso puede contener información falsa acerca del centro de coordinación. Tal como se examinó en la sección A, esto requiere que la entidad que quiera comprobar la autenticidad de un DIM tenga acceso a la lista de centros de coordinación que tiene que publicar periódicamente la OIT con arreglo al párrafo 4 del

artículo 4 del Convenio. Habida cuenta de que sólo hay unos cuantos centros de coordinación en funcionamiento, incluso en los países que han ratificado el Convenio núm. 185, esta lista aún no se ha publicado. Si se creara la entidad de coordinación de los centros de coordinación que se examinó en la opción A-6, se simplificaría mucho la distribución de información acerca de los centros de coordinación legítimos y las autoridades que quisieran comprobar la autenticidad de un DIM sólo tendrían que utilizar un sitio Web o llamar a un número de teléfono.

93. Aunque se creara una entidad de coordinación de centros de coordinación, para comprobar la autenticidad de un DIM se tendría que poder realizar una llamada internacional y comunicarse en un idioma que pudiera ser entendido por el personal del centro de coordinación o tener acceso a Internet para poder consultar el sitio Web del centro de coordinación. Debido a los posibles problemas con los idiomas, probablemente la mejor solución sea el acceso a Internet, aunque este acceso no siempre existe en los puertos o en los puestos fronterizos. Esto sugiere de nuevo que la mejor forma de comprobar la identidad de los marinos que llegan a los puestos fronterizos para embarcar en buques o desembarcar de ellos sería disponer de un punto de control secundario específico dotado de los dispositivos necesarios para verificar la identidad de los marinos y de una conexión a Internet a fin de autentificar los DIM. No obstante, existe otro método que puede funcionar bien cuando los marinos llegan a los puertos y solicitan poder disfrutar del permiso para bajar a tierra.

94. El párrafo 3 del artículo 6 del Convenio núm. 185 prevé que «la comprobación, las investigaciones y las formalidades mencionadas en el párrafo 2 *supra*, deberán efectuarse a la mayor brevedad, siempre que las autoridades competentes hayan recibido con tiempo suficiente el aviso de llegada del titular». Según la práctica establecida con arreglo al Convenio FAL, este aviso generalmente se proporciona antes de la llegada de un buque en forma de lista de tripulantes [23]. Una vez que se dispone de la lista de la tripulación, esta lista puede usarse en una ubicación central que tenga acceso a Internet para autentificar los DIM de todos los miembros de la tripulación a través del sitio web del centro de coordinación. Puede informarse a las autoridades competentes del puerto al que está previsto que llegue el buque del resultado de dicha autentificación.

95. El proceso de autentificar los DIM con antelación en base a la información que figura en la lista de la tripulación se vería considerablemente facilitado por el formato estándar de la lista de la tripulación de los buques y por la notificación previa [24]. De esta forma, la oficina que recibiera la lista podría autentificar cada DIM que figurara en ella a través de la entidad de coordinación de centros de coordinación o a través de diversos centros de coordinación y después enviar los resultados a las autoridades portuarias. Si se llegara a un acuerdo sobre un formato estándar de lista de la tripulación, podría preverse que la entidad de coordinación aceptara esas listas de la tripulación y enviara una respuesta estándar para cada marino que figurara en ellas, lo cual reduciría la carga de trabajo de la oficina que recibiera las listas de los buques antes de su llegada a puerto.

96. En la medida en que se consideren viables, las diversas opciones que figuran en esta sección B del documento podrían contribuir mucho a la seguridad en materia de admisión de marinos extranjeros en países que aún no pueden ratificar el Convenio núm. 185, y, en consecuencia, podrían facilitar la admisión de los marinos a fin de, entre otras cosas,

[23] Convenio FAL, anexo I (formulario FAL OMI 5), véase nota a pie de página 14.

[24] Quizá en relación con el concepto de ventanilla única para presentar información normalizada a un punto de entrada único, que actualmente se está examinando en la OMI, *ibíd*.

disfrutar del permiso para bajar a tierra, con arreglo al párrafo 2 de la regla 2.4 del MLC, 2006, y acceder a instalaciones de bienestar en tierra con arreglo a la regla 4.4.

97. La cooperación antes mencionada por parte de países que aún no han ratificado el Convenio núm. 185 también serviría para poner de relieve su compromiso con el bienestar de los trabajadores y con la facilitación del transporte marítimo mundial, así como con el objetivo básico del Convenio, que fue adoptado en 2003 por abrumadora mayoría y sin votos en contra.

Anexo I

Ratificaciones del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185)

(al 30 de noviembre de 2014)

País	Fecha	Estatus	Notas
Albania	11 de octubre de 2007	En vigor	
Azerbaiyán El 10 de abril de 2006, el Gobierno notificó que aplica provisionalmente el Convenio con arreglo a su artículo 9	17 de julio de 2006	No está en vigor	Aplicación provisional (artículo 9)
Bahamas	14 de diciembre de 2006	En vigor	
Bangladesh	28 de abril de 2014	En vigor	
Bosnia y Herzegovina	18 de enero de 2010	En vigor	
Brasil	21 de enero de 2010	En vigor	
Congo	14 de mayo de 2014	En vigor	
Croacia	6 de septiembre de 2011	En vigor	
Francia	27 de abril de 2004	En vigor	
Hungría	30 de marzo de 2005	En vigor	
Indonesia	16 de julio de 2008	En vigor	
Jordania	9 de agosto de 2004	En vigor	
Kazajstán	17 de mayo de 2010	En vigor	
Kiribati	6 de junio de 2014	En vigor	
Corea, República de	4 de abril de 2007	En vigor	
Lituania El 14 de agosto de 2006, el Gobierno notificó que aplica provisionalmente el Convenio con arreglo a su artículo 9	14 de agosto de 2006	No está en vigor	Aplicación provisional (artículo 9)
Luxemburgo	20 de septiembre de 2011	En vigor	
Madagascar	6 de junio de 2007	En vigor	
Islas Marshall	24 de agosto de 2011	En vigor	
Moldova, República de	28 de agosto de 2006	En vigor	
Nigeria	19 de agosto de 2004	En vigor	
Pakistán	21 de diciembre de 2006	En vigor	
Filipinas	19 de enero de 2012	En vigor	
Rusia, Federación de	26 de febrero de 2010	En vigor	
España	26 de mayo de 2011	En vigor	
Turkmenistán	12 de febrero de 2014	En vigor	
Vanuatu	28 de julio de 2006	En vigor	
Yemen	6 de octubre de 2008	En vigor	

Anexo II

Partes seleccionadas de la norma ISO/IEC 24713-3:2009 [1]

Cabe señalar que, con fines de referencia, en los extractos que figuran a continuación ISO/IEC 7501 es la versión de la ISO del documento núm. 9303 de la OACI, que contiene exactamente el mismo texto que el documento de la OACI pero permite que en otras normas de la ISO se haga referencia a él.

[1] Se trata de un extracto de un documento técnico elaborado por la ISO que sólo está disponible en inglés.

1 Scope

This part of ISO/IEC 24713 specifies a biometric profile including data interchange formats, system requirements, and the operation of biometric procedures on a Seafarers' Identity Document (SID).

Note that the domain of applicability may extend to other situations where an interoperable biometrics-based identity document is required, but the main focus is on the use of biometrics on a Seafarers' Identity Document (SID).

This part of ISO/IEC 24713 notes that ILO Convention No. 185 already provides the overarching policy guidance on biometric verification and identification of seafarers and it relies on that guidance. Determining any matters of policy beyond those or in contradiction to those included in ILO Convention No. 185 is explicitly out of scope for this standard.

...

6 Application requirements

6.1. General

The requirements of a globally interoperable system of seafarers' identity documents to be used for the biometric verification and identification of seafarers are outlined in this clause. The requirements focus on the biometric aspects of this application, but where other aspects affect the use of biometrics, they are also discussed. These requirements are intended to be in accordance with the regulatory requirements of the Seafarers' Identity Documents Convention (Revised), 2003 (No.185) [3] and to ensure backwards compatibility with the existing practices of the ILO and with SIDs already issued. There are currently several requirements of the existing Convention that would be difficult to change and which this standard normatively requires for all verification and identification of seafarers. Permission has been given for certain portions of Convention No. 185 to be quoted directly in this document, and these are used to help define the requirements. The relevant sections of Convention No. 185 (renumbered to make sense when quoted without the full text of the Convention) follow in Clause 6.2.

6.2 Requirements of ILO SID convention

6.2.1 Physical composition of the document

The seafarers' identity document shall be designed in a simple manner, be made of durable material, with special regard to conditions at sea and be machine-readable. The materials used shall:

a) prevent tampering with the document or falsification, as far as possible, and enable easy detection of alterations; and

b) be generally accessible to governments at the lowest cost consistent with reliably achieving the purpose set out in (a) above.

NOTE 1 This requirement comes from Article 3, paragraph 2 of Convention No. 185 [3].

NOTE 2 The specific details associated with this requirement are found by reference to the physical layout and document specifications for either a TD-3 booklet size document as defined in ISO/IEC 7501-1 or preferably a TD-1 card size document as defined in ISO/IEC 7501-3.

6.2.2 Personal data contained in the document

Particulars about the holder included in the seafarer's identity document shall be restricted to the following:

c) full name (first and last names where applicable);

d) sex;

e) date and place of birth;

f) nationality;

g) any special physical characteristics that may assist identification;

h) digital or original photograph; and

i) signature

NOTE This requirement comes from Article 3, paragraph 7 of Convention No. 185 [3].

6.2.3 Biometric data contained in the document

Notwithstanding 6.2.2 above, a template or other representation of a biometric of the holder shall also be required for inclusion in the seafarers' identity document, provided that the following preconditions are satisfied:

a) the biometric can be captured without any invasion of privacy of the persons concerned, discomfort to them, risk to their health or offence against their dignity;

b) the biometric shall itself be visible on the document and it shall not be possible to reconstitute it from the template or other representation;

NOTE This requirement is interpreted to mean that the fingerprint template which is a representation of the biometric used in the document shall be made visible by being encoded in a two dimensional barcode. Since the ISO 19794-2 fingerprint template profiled in this standard is a representation only of bifurcations and endpoints, this is interpreted to be only a subset of the information in the original biometric characteristic of the fingerprint and thus satisfies the requirement that the biometric can not be reconstituted from the template.

c) the equipment needed for the provision and verification of the biometric is user-friendly and is generally accessible to governments at low cost;

d) the equipment for the verification of the biometric can be conveniently and reliably operated in ports and in other places, including on board ship, where verification of identity is normally carried out by the competent authorities; and

e) the system in which the biometric is to be used (including the equipment, technologies and procedures for use) provides results that are uniform and reliable for the authentication of identity.

NOTE This requirement comes from Article 3, paragraph 8 of Convention No. 185 [3].

6.2.4 Visibility of data

All data concerning the seafarer that are recorded on the document shall be visible. Seafarers shall have convenient access to machines enabling them to inspect any data concerning

them that is not eye-readable. Such access shall be provided by or on behalf of the issuing authority.

NOTE This requirement comes from Article 3, paragraph 9 of Convention No. 185 [3]

6.2.5 Secure electronic database

Each Member shall ensure that a record of each seafarers' identity document issued, suspended or withdrawn by it is stored in an electronic database. The necessary measures shall be taken to secure the database from interference or unauthorized access.

NOTE 1 This requirement comes from Article 4, paragraph 1 of Convention No. 185 [3]

NOTE 2 The detailed contents of this database are described elsewhere in Convention No. 185 [3], but for purposes of this standard they are defined in Clause 6.5.4 of this document

NOTE 3 There will usually be a separate issuance database created by the document issuance system that is used to record personal information and issue the SID, but this is not specified either in Convention No. 185 [3] or in this part of ISO/IEC 24713

6.2.6 Restrictions on database content

The information contained in the record shall be restricted to details which are essential for the purposes of verifying a seafarers' identity document or the status of a seafarer and which are consistent with the seafarer's right to privacy and which meet all applicable data protection requirements.

NOTE This requirement comes from Article 4, paragraph 2 of Convention No. 185 [3]

6.2.7 Access to the database

Each Member shall designate a permanent focal point for responding to inquiries, from the immigration or other competent authorities of all Members of the Organization, concerning the authenticity and validity of the seafarers' identity document issued by its authority. Details of the permanent focal point shall be communicated to the International Labour Office, and the Office shall maintain a list which shall be communicated to all Members of the Organization.

The details referred to in paragraph 6.2.5 above shall at all times be immediately accessible to the immigration or other competent authorities in member States of the Organization, either electronically or through the focal point referred to above.

NOTE This requirement comes from Article 4, paragraphs 4 and 5 of Convention No. 185 [3].

6.2.8 Data protection and privacy

For the purposes of this Convention, appropriate restrictions shall be established to ensure that no data - in particular, photographs - are exchanged, unless a mechanism is in place to ensure that applicable data protection and privacy standards are adhered to.

Members shall ensure that the personal data on the electronic database shall not be used for any purpose other than verification of the seafarers' identity document.

NOTE This requirement comes from Article 4, paragraphs 6 and 7 of Convention No. 185 [3].

…

6.5 Data storage formats and data storage media

6.5.1 General

There are privacy concerns about storing images of fingerprints that may hinder adoption of a system based on fingerprint images. Individual documents will also be more expensive if fingerprint images are used because of the additional data storage requirements.

For these reasons, the format for storing fingerprints in a seafarers' identity document shall be one of those defined in ISO/IEC 19794-2 Information Technology – Biometric Data Interchange Formats – Part 2: Finger Minutiae Data.

Since existing practice is to display photographs on seafarers' identity documents, there should not be any privacy issues with using face images. Therefore the storage format for face images shall be ISO/IEC 19794-5 Information Technology – Biometric Data Interchange Formats – Part 5: Face Image Data.

Although all SIDs created prior to publication of this part of ISO/IEC 24713 were based on earlier ILO documents and use a data format for fingerprint minutiae records based on an older draft of ISO/IEC 19794-2 as profiled in detail in ILO SID-0002, it should be possible in the future for parsers to identify whether the record is an old record or a new record based on the header bytes and to interpret the remainder of the record appropriately. Therefore the requirement for backwards compatibility does not restrict this standard from using the final published versions of the data formats and all systems and documents claiming conformance to this standard for issuance of SID cards shall use only those versions of the data formats profiled in Clause A.6 of this standard. The only constraints should be the memory capacity of the media being used to store the data and the ability to achieve the interoperable performance outlined in Clause 6.4. It is, however, recommended but not required that systems conforming to this standard for verification should also support biometric matching using the older fingerprint minutiae format profiled in ILO SID-0002.

Biometric data used for the verification and identification of seafarers in the context of this standard will be stored both in a secure electronic database (as described in Clause 6.2.5) and on an identity document. All SIDs that are compliant to ILO Convention No. 185 use a PDF 417 bar code to store an ISO/IEC 19794-2 record containing minutiae data from two fingers and therefore all SIDs that are conformant to this standard shall include such a barcode, as defined in ISO/IEC 15438.

6.5.2 Two dimensional bar code

In order to make the bar code legible, it should be printed as large as is practical within the allotted space on the document. The available space is defined by the ID-1 size card layout in ISO/IEC 7501-3 (for SIDs that are cards) and by the passport data page layout in ISO/IEC 7501-1 (for SIDs that are in ID-3 size booklet form). This determines the space that remains for additional print features once all of the mandatory features, such as the seafarer's printed photograph and the document's machine readable zone, have been printed. The specific positioning of the two dimensional barcode depends on the document size.

For ID-3 size booklets, the bar code shall be placed immediately to the right of the printed photograph of the seafarer (Zone V in ISO/IEC 7501-1) and immediately above the machine readable zone (Zone VII in ISO/IEC 7501-1). In order to leave space for other necessary data elements the area allotted for the two dimensional bar code including all necessary quiet zones shall not be more than 21.35 mm in height and it shall not extend below 23.2 mm above the bottom of the document since the first 23.2 mm are allotted to the machine readable zone. The bar code shall also be limited in width by the end of the printed photograph in Zone V on the left side and the 2 mm no-print zone at the edge of the document on the right side. Since the width of the photograph is somewhat flexible in ISO/IEC 7501-1, it is not possible to specify an exact width for the bar code.

For ID-1 size cards, the bar code shall be printed on the reverse side of the card from the printed photograph and shall be printed at the top of this side of the card, with the machine readable zone printed at the bottom. The two dimensional bar code shall be printed entirely within Zone VI as defined in ISO/IEC 7501-3 and therefore the maximum size of the two dimensional barcode shall be 85.6 mm in width and 27.8 mm in height including all necessary quiet zones.

In order to permit the finger minutiae data to be stored in the limited space available on a two dimensional bar code, the only data contained in the bar code shall be a template containing two finger minutiae data records of CBEFF format type 3 or CBEFF format type 4, as defined in ISO/IEC 19794-2 and profiled in Clause A.6.2 of this standard. This template shall be wrapped in a CBEFF Patron Format Header specified in Annex B and a CBEFF Security Block specified in Annex C. This use of the CBEFF Patron Format and Security Block is profiled in clause A.6.4.

The data contained within the two dimensional barcode shall be encoded and printed using the PDF 417 bar code symbology specification defined in ISO/IEC 15438. The precise size of the bar code data symbols as well as the number of rows and columns should be decided by the authority that prints the document based on the size of the document and the print technology used to create it. The only mandatory requirement is that an error correction level of 5 shall be used and the barcode shall be readable with commercial hand held barcode readers. One recommended option is to use an x-dimension for the bar code data symbols of 0.170 mm and a y-dimension of 0.511 mm.

…

6.5.4 Secure electronic database

The secure electronic database maintained by each ILO member state that issues SIDs shall store key data (See Table 1) from each SID issued by that state and shall make it available to SID verification authorities that may have cause to enquire about specific SIDs or seafarers as required in Clause 6.2.7. The secure electronic database is required to maintain records of each document issued, suspended or withdrawn and to maintain enough information to allow verification of individual SIDs or of the status of a particular seafarer. Access to this information shall be given to properly authenticated verification authorities, provided that the security mechanisms in place for the verification authorities are secure against accidental or unprotected disclosure. This can be accomplished using the security techniques outlined in Clause 6.6. The secure electronic database shall also store logs of the verification enquiries made against each SID record that it contains and it is recommended that these logs be retained for a minimum of ten years subject to national legislative requirements.

Any document issuance system used to create and issue SIDs is likely to have a large database containing a full record of every seafarer, every document issued, all of the information used during the issuance process and audit logs of all actions taken concerning each seafarer and document. Such databases are typically proprietary solutions that depend on the particular issuance software and procedures used by each SID issuing authority. They may also be affected by individual jurisdictional requirements about such issues as whether or not complete ten-fingerprint sets are acquired from seafarers as part of the security check during the enrolment process and, if so, whether these fingerprint images are retained or deleted after security checks have been completed.

The secure electronic database defined in this standard shall be separate from any proprietary issuance database (using either physical or electronic separation) and shall only contain the data for each SID that is explicitly listed in this Clause, as this is considered sufficient to satisfy the requirement to allow verification of SIDs and seafarers. These data elements are listed in the Table below with an indication of whether they are mandatory or optional and a historical indication of whether they are present in currently deployed SID systems that use ILO technical documents published prior to the development of this standard.

Item No	Data Element	Data Description	Mandatory or Optional	Present in Legacy SID Electronic Databases
1	Issuing authority named on the identity document	Variable Length Text String containing the three character ISO code (see ISO/IEC 7501-1) for the issuing state and the name and full address of the SID issuing authority as well as the name and position of the person authorizing the issue	Mandatory	Yes
2	Full name of seafarer as written on the identity document	Variable Length Text String containing the full name of the seafarer	Mandatory	Yes
3	Unique document number of the identity document	12 Character Text String containing the three character ISO code (see ISO/IEC 7501-1) for the issuing state followed by a nine character document identity number that is unique among all SIDs issued by the SID issuing authority in that state	Mandatory	Yes
4	Date of expiry or suspension or withdrawal of the document	10 Character Text String (ASCII encoded) containing a date of expiry, suspension or withdrawal of the document in the format (dd/mm/yyyy)	Mandatory	Yes
5	Status of document termination date	1 Character Text String (ASCII encoded) indicating the meaning of the date field described in data element 4. This is set to: D – Date is date of expiry of document S – Date indicates date on which document was suspended W – Date is date on which document was withdrawn	Mandatory	No
6	Fingerprint template appearing on the identity document	Variable Length Binary containing the two fingerprint 19794-2 minutiae record encapsulated in a CBEFF record containing a security block exactly as encoded in the two dimensional barcode in the SID and described in Clause 6.5.2 of this standard.	Mandatory (unless prohibited by legislative requirements)	Yes May be in 19794-2 format profiled in ILO SID-0002
7	Face image appearing on the identity document	Variable Length Binary containing the facial image that is printed as the photograph on the physical SID contained within a 19794-5 face image record as profiled in Clause A.6.3 of this standard and using a CBEFF header and Security Block as profiled in Clause A.6.4 of this standard.	Mandatory	Yes May be simple image without 19794-5 format
8	Fingerprint images corresponding to the minutiae record of two fingers stored in the identity document'	Variable Length Binary containing the two fingerprint images that correspond to the two fingers present in the minutiae record present in the two dimensional barcode on the document. These images shall be encoded in a single 19794-4 fingerprint image record as profiled in Clause A.6.1 of this standard.	Optional	No
9	Details of all inquiries made	Internal database logs recording the identity of the verification authority making each inquiry, the details	Mandatory	Yes

Item No	Data Element	Data Description	Mandatory or Optional	Present in Legacy SID Electronic Databases
	concerning the seafarers' identity document	used to validate that verification authority, the date and time of the query and the unique document number of the SID against which the enquiry was made. The internal format used to record this information is up to each issuance authority as this information is not for exchange but for providing audit reports to issuance authorities and, for queries against their own SID, to seafarers.		

Table 1 — Data Elements in the Secure Electronic Database

In order to address privacy and data security concerns, these data elements should be protected and shall not be released except to authenticated verification authorities using the procedures outlined in Clause 6.8.

…

A.6.4 ISO/IEC 19785 (CBEFF)

Annexes B and C provide further information on the CBEFF Patron format and Security Block that are profiled here. The maximum length of a CBEFF record profiled in accordance with this clause and used with a BDB consisting of a two finger minutiae record profiled in accordance with Clause A.6.2 is 635 bytes. This consists of 3 bytes for the Standard Biometric Header, a maximum of 556 bytes for the two finger minutiae record, and 76 bytes for the Security Block. The references in this profile are not to the ISO/IEC 19785 multi-part standard, but to the Annexes B and C in this part of ISO/IEC 24713 which provide the description of the CBEFF Patron Format and Security Block defined for use with Seafarers' Identity Documents. Detailed explanations of the meaning of the various parts of the CBEFF Patron format can be found in ISO/IEC 19785-1 and ISO/IEC 19785-3.

Base Standard Requirements List						Profile Requirements List and Implementation Conformance Statement			
Item	Section	Operator	Operands	Base Ref.	Status	Operator	Operands	Status	Support
	Annex B Patron Format (Standard Biometric Header)								
1	CBEFF_BDB_format_owner	EQ	0-65535	B.10.1	M	EQ	0 (Indicates 257 for ISO/IEC JTC 1 SC 37)	M	1 bit
2	CBEFF_BDB_format_type	EQ	0-65535	B.10.1	M	EQ	0b0000011 or 0b0000100	M	7 bits
3	Reserved bits	EQ	0	B.10.1	M	EQ	0b0000	M	4 bits
4	Length of BDB			B.10.1	M	EQ	36-556	M	12 bits
5	BDB			B.10.1	M			M	
	Annex C Security Block								
6	SID Issuing Authority	C	See NOTE 1	C.1	M	C	See NOTE 1	M	3 bytes
7	Unique document number	C	See NOTE 2	C.1	M	C	See NOTE 2	M	9 bytes
8	Signature	C	See NOTE 3	C.1	M	C	See NOTE 1	M	64 bytes

NOTE 1 The three bytes form a three character string that is present in the visual zone of the SID and corresponds to the ISO code of the country of the issuing authority. The string represented by these three bytes shall correspond to that printed in the visual zone and in characters 3 through 5 of the first line of the machine readable zone (MRZ).

NOTE 2 The nine bytes in this field form a nine character string that is present in the visual zone of the SID as the SID number (excluding the three character ISO country code). The string represented by these three bytes shall correspond to that printed in the visual zone, with leading zeros if the SID number in the visual zone is less than nine characters in length.

NOTE 3 The signature shall use SHA-256 for hashing and ECDSA for signing, as explained in Annex C below.

Annex B
CBEFF patron format for the SID
(normative)

B.1 Patron

ISO/IEC JTC 1/SC 37

B.2 Patron identifier

257 (0101Hex). This has been allocated by the Registration Authority for ISO/IEC 19785-2.

B.3 Patron format name

ISO/IEC JTC 1/SC 37 Patron format for Seafarers Identity Document

B.4 Patron format identifier

9 (0009 Hex). This has been registered in accordance with ISO/IEC 19785-2.

B.5 ASN.1 object identifier for this patron format

```
{iso registration-authority cbeff(19785) biometric-organization(0) jtc1-sc37(257) patron-format(1) sid(9)}
```

or, in XML value notation,

```
1.1.19785.0.257.1.9
```

B.6 Domain of use

This Annex contains the definition of a minimum patron format for simple BIR structures that has been designed for use with seafarers' identity documents, but may be of general utility in domains of use that wish to minimise the overhead of the SBH in order to reduce storage or transfer bandwidth and processing costs at the expense of information content, that are able to accept some loss of byte alignment, and that need to support INTEGRITY with no ENCRYPTION. A suitable CBEFF Security Block is defined in Annex C.

B.7 Version identifier

This patron format specification has a version identifier of (major 0, minor 0).

B.8 CBEFF version

This specification conforms to CBEFF version (major 2, minor 0).

B.9 General

This clause defines a minimum conforming patron format. The formal specification of this Patron Format is provided using the ASN.1 notation (see ISO/IEC 8824-1) together with the specification of the ASN.1 Packed Encoding Rules (ISO/IEC 8825-2).

The Patron format for seafarers' identity documents is formally defined as the ASN.1 PER-unaligned encoding rules applied to the SID-format type specified in B.10.1

An example of the encoding produced by an assignment of abstract values for this patron format, showing the size and encoding of each field of the SBH, is given in table B.1. The size of the SBH is three bytes if

a) the BDB format is standardized by SC 37, with a format type value less than 64; and

b) the BDB length is less than 2048 bytes.

The size can be greater if these constraints are not satisfied.

NOTE The data format selected for use in the two dimensional barcodes in SIDs and described in this standard ensures that these constraints are satisfied.

Table B.1— SID Patron format SBH (3 bytes)

Format owner is SC 37?	Format type is <64?	Format type value	Reserved	Length of BDB is less than 2048 bytes?	Length of BDB
one bit	one bit	6 bits	4 bits	one bit	11 bits
set to zero if Format owner is SC 37	set to zero if Format type is less than 64	will be longer if format type is 64 or greater (which is not possible in this version of the profile)	pads the SBH to exactly 3 bytes for this version of the profile	set to zero if the BDB Length is less than 2048 bytes	will be longer if BDB Length is 2048 bytes or greater (which is not possible in this version of the profile)

B.10 Bit oriented patron format specification and conformance statement

The detailed specification of the patron format and the list of mandatory and optional data elements are described in the following clauses.

B.10.1 Specification

The following notation is specified in ISO/IEC 8824-1. The data type shall be encoded in accordance with the UNALIGNED version of BASIC-PER (see ISO/IEC 8825-1).

```
CBEFF-SID-PATRON-FORMAT {iso standard 24713 sid (3) modules(0) patron-
format(0)}
        -- This module is 1.0.24713.3.0.0 for entry into the module
database
DEFINITIONS
AUTOMATIC TAGS ::=
BEGIN

IMPORTS SID-Security-Block FROM SID-SECURITY-BLOCK {iso standard 24713
sid (3) modules(0) security-block(1)};

SID-format ::= SEQUENCE {
      /* This patron format contains only mandatory data elements and
      uses bit-level encoding for optimal use of encoding space.*/
      /* This patron format supports only the abstract values NO
      ENCRYPTION and INTEGRITY, which are encoded as zero length
      fields.*/
      /* This patron format supports only the security block
         {iso registration-authority cbeff(19785) biometric-
      organization(0) jtc1-sc37(257) SB-formats(2) sid(3)} specified in
      Annex C*/

      bdb-format  SEQUENCE {
                        owner       INTEGER (0..65535) DEFAULT 257,
                              -- 257 is the biometric organization
      identifier of ISO/IEC JTC 1/SC 37.  Encodes in 1 bit if 257.
                        type        INTEGER (0..63, ..., 64..65535)},
                              -- Encodes in 7 bits for CBEFF identifiers
      less than 64.

      reserved    BIT STRING (SIZE (4))('0000'B),
                              -- Encodes in 4 bits, all set to zero in
this version

      sb-format   SEQUENCE {
                        owner       INTEGER (257)  /* Null encoding*/,
                        type        INTEGER (3)    /*Null encoding*/ },

      bdb         OCTET STRING (SIZE(0..2047, ..., 2048 .. MAX)),
                              -- Encodes in 12 bits plus the length of
the BDB

      sb          SID-Security-Block }

END
```

B.11 Patron format conformance statement

The following tables provide the list of mandatory elements for this patron format.

B.11.1 Identifying information

Required Information	Patron format reference
Patron name	See B.1
Patron identifier	See B.2
Patron format name	See B.3

Required Information	Patron format reference
Patron format identifier	See B.4
Patron format ASN.1 object identifier	See B.5
Domain of use description	See B.6
Patron format version	See B.7
CBEFF version	See B.8

B.11.2 CBEFF-defined data elements and abstract values

CBEFF data element name	Mandatory/ optional	Patron format field name	Abstract values specified?	Encodings specified?
CBEFF_BDB_format_owner	Mandatory	owner	Yes	Yes
CBEFF_BDB_format_type	Mandatory	type	Yes	Yes
CBEFF_BDB_encryption_options	Mandatory	zero length field	Yes	Yes
CBEFF_BIR_integrity_options	Mandatory	zero length field	Yes	Yes
CBEFF_SB_format_owner	Mandatory	zero length field	Yes	Yes
CBEFF_SB_format_type	Mandatory	zero length field	Yes	Yes

B.11.3 Patron defined data elements and abstract values

Patron format data element name	Mandatory/ optional	Patron format field name	Abstract values specified?	Encodings specified?
None	n/a	n/a	n/a	n/a

Annex C
CBEFF security block for the SID
(normative)

C.1 Introduction

This Security Block (SB) is designed for use in a Seafarers' Identity Document, but it could be more widely used for other documents with limited storage for biometric data. It provides integrity and source authentication by implementing digital signatures. It accomplishes a minimal size by making use of the Elliptic Curve Digital Signature Standard (ECDSA) and a binary encoding of the resulting signature and an algorithm identifier. It specifies the algorithm identifiers and encoding rules for ECDSA digital signatures when using SHA-256 as the hashing algorithm. The reference documents for these algorithms are the draft Federal Information Processing Standard (FIPS) "Draft Secure Hash Standard" [1], the draft FIPS "Draft Digital Signature Standard" [2], and X9.62-2005, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA)" [8]. The SB contains:

a) the three character country code (see ISO/IEC 7501-1) of the issuing authority for the card, encoded in ASCII (3 bytes);

b) a nine digit identification encoding the document number which is unique among all documents issued by the SID issuing authority for that country, encoded in ASCII (9 bytes);

NOTE The combination of items a) and b) forms a globally unique document identity number for a particular SID which can be used to look up, using secure out-of-band mechanisms, all the parameters, particularly the public key of the issuing authority that was used to create a particular SID, needed to validate the digital signature contained in the Security Block. The details of these out-of-band mechanisms are not in the Scope of this part of ISO/IEC 24713, and will be determined by individual bilateral agreements between verification authorities and SID issuing authorities or between verification, authorities, issuing authorities and a central focal point coordination centre controlled by the ILO as described in Clause 6.8.3. It is expected that this information will be obtained regularly, and will be cached as necessary for offline verification of SIDs.

c) the digital signature (64 bytes)

Signature algorithms are always used in conjunction with a one-way hash function. In this security block, the CBEFF BIR to be signed (the SBH and the BDB), is processed by the SHA-256 hash function, creating an output value of length 256 bits (32 bytes). This output value is then formatted for signing by the ECDSA algorithm. When signing, the ECDSA algorithm generates two values commonly referred to as r and s. To create a signature value, they are concatenated as follows:

signature = r, s

This binary signature value becomes the Signature Field.

Each of the components of the signature (r and s) are equal in size to the key length (32 bytes or 256 bits).

Thus: SHA-256 with elliptic key encoding with a key length of 256 bits gives a hash size of 32 bytes and a signature size of 64 bytes.

More detail on how digital signatures are generated can be found in [2].

C.2 SB owner

ISO/IEC JTC 1/SC 37

C.3 SB owner identifier

257 (0101Hex). This has been allocated by the Registration Authority for ISO/IEC 19785-2.

C.4 SB format name

ISO/IEC JTC 1/SC 37 security block format for Seafarers Identity Document

C.5 SB format identifier

3 (0003 Hex). This has been registered in accordance with ISO/IEC 19785-2.

C.6 ASN.1 object identifier for this SB format

```
{iso registration-authority cbeff(19785) biometric-organization(0) jtc1-
sc37(257) sb-format(1) sid(3)}
```

or, in XML value notation,

```
1.1.19785.0.257.1.3
```

C.7 Version identifier

This security block format specification has a version identifier of (major 0, minor 0).

C.8 SB specification

The following notation is specified in ISO/IEC 8824-1. The data type shall be encoded in accordance with the UNALIGNED version of BASIC-PER (see ISO/IEC 8825-1).

```
SID-SECURITY-BLOCK {iso standard 24713  sid (3) modules(0) security-
block(1)}
-- This module is 24713.3.0.1 for entry into the module database
DEFINITIONS
AUTOMATIC TAGS ::=
BEGIN

SID-Security-Block ::= SEQUENCE {
      sid-issuing-authority  IA5String (SIZE(3)),
                             -- This is the ISO/IEC 7501-1 3-digit
      Country Code of the issuing authority
      unique-document-number IA5String (SIZE(9)),
                             -- Unique for this issuing authority.
      Used to determine security algorithm parameters by out-of-band
      means
      signature-r            OCTET STRING (SIZE(32)) ,
      signature-s            OCTET STRING (SIZE(32))
                             -- The content of the signature is
      specified in C.1 -- }

END
```

C.9 Size of the SB encoding

`sid-issuing-authority`	3 bytes
`unique-document-number`	9 bytes
`signature-r`	32 bytes
`signature-s`	32 bytes

The total is 76 bytes

Note that the `sid-issuing-authority` and `unique-document-number`.are needed to recover the public key of the issuing authority for that particular SID or, more typically, for a series of SIDs that includes the SID currently being verified.